UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

La conjetura de Erdös-Straus

Autor/es

JAVIER OCHOA GONZÁLEZ

Director/es

MANUEL BELLO HERNÁNDEZ

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2017-18

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

FACULTAD DE CIENCIAS Y TECNOLOGÍA

Departamento de Matemáticas y Computación

TRABAJO DE FIN DE GRADO 2017-2018

La conjetura de Erdös-Straus

GRADO EN MATEMÁTICAS

Alumno: JAVIER OCHOA GONZÁLEZ

Tutor: MANUEL BELLO HERNÁNDEZ

Logroño, Junio del 2018

Resumen

Este trabajo pretende aportar al lector una amplia perspectiva de la conjetura de Erdös-Straus. Se incide en el conocimiento sobre la estructura básica de los números naturales, ya que la conjetura está relacionada con las propiedades aditivas y multiplicativas de estos. Además, se estudian distintas cuestiones de combinatoria, estructuras algebraicas, teoría de números, topología y análisis complejo.

Tras una primera sección donde se motiva el estudio de la conjetura, se estudia la representación de una fracción racional como suma de dos fracciones con numerador igual a uno. Además, se observa que cuando los denominadores de las fracciones son potencias de un número primo impar, el conjunto de los denominadores de dichas fracciones para los que no hay tales descomposiciones es un subgrupo con propiedas interesantes.

En la sección 3, se presenta la conjetura de Erdös-Straus, caracterizando también los números para los que la conjetura es cierta. Estas caracterizaciones ayudan a construir un polinomio cuyos valores satisfacen la conjetura. En la sección 4, se comprueba que los cuadrados perfectos no están contenidos en la imagen de dicho polinomio; para ello, se requiere la utilización del teorema de reciprocidad cuadrática de Gauss. La sección 5 continúa viendo propiedades de estos números: en particular, se comprueba la densidad del conjunto de dichos números. Para la prueba de esto, se da un teorema de Landau sobre la distribución asintótica de los números que se pueden expresar como suma de dos cuadrados, y se dan algunas ideas para su demostración. Estas ideas se completan con las notas adicionales, donde incluimos resultados necesarios para la prueba del teorema.

Abstract

This work seeks to contribute a wide perspective of the Erdös-Straus conjecture to the reader. It is focused on the knowledge on the basic structure of the natural numbers, since the conjecture is related to the additive and multiplicative properties of these. Also, different questions about combinatory, algebraic structures, theory of numbers, topology and complex analysis are studied.

After a first section where the study of the conjecture is motivated, the representation of a rational fraction is studied as supreme of two fractions with numerator similar to one. Also, it is observed that when the denominators of the fractions are powers of a odd prime number, the set of the denominators of this fractions for those that there is no possible decomposition is a subgroup with interesting properties.

In the section 3, the Erdös-Straus conjecture is presented, also characterizing the numbers for those that the conjecture is certain. These characterizations help to build a polynomial whose values satisfy the conjecture. In the section 4, it is proven that the perfect squares are not contained in the image of this polynomial; for it, the use of the theorem of quadratic reciprocity of Gauss is required. The section 5 continues to see some properties of these numbers: in particular, it is proven the density of one group of this numbers. For the test of this, a theorem of Landau is given on the asymptotic distribution of the numbers that can be expressed like it adds of two squares, and some ideas are given for their demonstration. These ideas are completed with the additional notes, where we include necessary results for the proof of the theorem.

Índice

1. Introducción

En la actualidad, estamos acostumbrados a escribir números como decimales o fracciones. La representación de coma flotante utilizada en los ordenadores es también una representación muy similar a los decimales.

Los antiguos egipcios utilizaron un sistema numérico basado en *fracciones unitarias*: fracciones de la forma $\frac{1}{n}$.

Esta idea les permitía representar números como $\frac{1}{7}$ con bastante facilidad; otros números como $\frac{2}{7}$ se representaban como suma de fracciones unitarias (por ejemplo, $\frac{2}{7} = \frac{1}{4} + \frac{1}{28}$). Además, en ese sistema numérico, la misma fracción no podría usarse dos veces (por lo tanto, $\frac{2}{7} = \frac{1}{7} + \frac{1}{7}$ no está permitido).

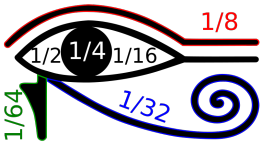


Figura 1: El ojo de Horus (*Udyat*) contiene los símbolos jeroglíficos de los primeros números racionales.

El papiro de Ahmes, también conocido como papiro matemático Rhind, es uno de los escritos matemáticos más antiguos que conocemos. A lo largo de sus seis metros de longitud por 32 cm de anchura, hay diversos problemas; en particular, problemas que tratan de la representación de números racionales (fracciones de la forma $\frac{m}{n}$) como suma de k fracciones unitarias:

$$\frac{m}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k}$$

Actualmente todavía hay estudios implicados en resolver este tipo de problemas. Prácticamente cada estudio sugiere un método distinto de conversión, cada uno con sus ventajas y desventajas.

Esto ha sugerido, y sigue sugiriendo, numerosas conjeturas, muchas de los cuales todavía no han sido resueltas. En [3] y [4] podemos encontrar diversos algoritmos propuestos para construir representaciones de fracciones como el algoritmo de Fibonacci-Sylvester, el algoritmo de las sucesiones de Farey y el algoritmo de fracciones continuas. En [9] también encontramos diversos problemas sobre estas fracciones propuestos por Erdös y Graham.

Figura 2: El papiro de Ahmes, también conocido como papiro matemático Rhind

Una de las conjeturas más famosas, y en la que centraremos el estudio, es la Conjetura de Erdös-Straus, que establece que, *dado un número entero positivo* $n \geq 2$*, existen* $x,\ y,\ z \in \mathbb{N}$ *tales que*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}. \tag{1.1}$$

En caso de que existan tales x, y, z, decimos que n es un número de Erdös-Straus y nos referimos a (1.1) como la descomposición de Erdös-Straus de $\frac{4}{n}$. Wacław Sierpiński y Andrzej Schinzel proponen una versión generalizada de la conjetura, que dice que, *para cualquier* k *positivo, existe un número* $N \in \mathbb{N}$ *tal que, para todo* $n \geq N$*, hay al menos una solución para* $\frac{k}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ *con* x*,* y*,* z *enteros positivos.*

Las raíces de estas conjeturas están en la búsqueda del número mínimo de fracciones unitarias necesarias para descomponer una fracción de la forma $\frac{m}{n}$ como la suma de dos fracciones unitarias. Matemáticos como Bernstein, Elsholtz, Swett, Tao, Yamamoto, etc. han intentado resolver la conjetura, aunque sin éxito, ya que no se ha logrado probar el caso general $\forall n \in \mathbb{N}$. Salez comprobó en 2014 la conjetura para todo $n \leq 10^{17}$.

Si n es un número de Erdös-Straus, entonces la conjetura también se cumple para todo $m \in \mathbb{N}$ múltiplo de n. Esto nos lleva a que la conjetura debería comprobarse solo para números primos de la forma $n = 4q + 1$; ya que, $\forall q \in \mathbb{N}$ se cumple $\frac{4}{4q+3} = \frac{1}{q+1} + \frac{1}{(q+1)(4q+3)}$. Además si n admite la factorización $n = abc$, tenemos la descomposición

$$\frac{1}{n} = \frac{1}{a(a+b)c} + \frac{1}{b(a+b)c}.$$

2. Descomposición en dos fracciones egipcias

2.1. La existencia de descomposición

Uno de los primeros problemas que nos planteamos es saber cuando podemos descomponer una fracción de la forma $\frac{m}{n}$ con $m, n \in \mathbb{N}$ como suma de dos fracciones unitarias. En esta sección damos solución a este primer problema.

Por ejemplo, resulta evidente que podemos expresar cualquier fracción de la forma $\frac{2}{n}$ como suma de dos fracciones unitarias $\forall n \in \mathbb{N}$, pero no podemos asegurar lo mismo para $\frac{3}{n}$. La ecuación $\frac{3}{n} = \frac{1}{x} + \frac{1}{y}$ tiene solución $x, y \in \mathbb{N}$ si y solo si n tiene un divisor m de la forma $m \equiv 0$ ó $m \equiv 2 \pmod 3$, lo que es equivalente a $\frac{3}{n} = \frac{1}{x} + \frac{1}{y}$ tiene solución si y solo si n tiene un divisor m que no es congruente con 1 módulo 6. Para probar esto con rigor, veamos dos resultados donde daremos las condiciones necesarias para descomponer una fracción de la forma $\frac{m}{n}$ como suma de dos fracciones unitarias.

Lema 2.1. *La fracción $\frac{m}{n}$ (con m, n no necesariamente primos entre sí) se puede descomponer como suma de dos fracciones unitarias si y solo si existen k_1, $k_2 \in \mathbb{N}$ tales que*

$$k_1 k_2 = n^2 \tag{2.1}$$

$$m|(n + k_1),\ m|(n + k_2). \tag{2.2}$$

Demostración. Si se cumplen las condiciones (2.1) y (2.2), se tiene que $a = (n + k_1)/m$, $b = (n + k_2)/m$ cumplen:

$$\begin{aligned}\frac{1}{a} + \frac{1}{b} &= m\left(\frac{1}{n + k_1} + \frac{1}{n + k_2}\right) = m\left(\frac{2n + k_1 + k_2}{n^2 + (k_1 + k_2)n + k_1 k_2}\right) \\ &= m\left(\frac{2n + k_1 + k_2}{n(2n + k_1 + k_2)}\right) = \frac{m}{n}.\end{aligned}$$

Por otra parte, si $\frac{m}{n} = \frac{1}{a} + \frac{1}{b}$, entonces $k_1 = am - n \in \mathbb{N}$, $k_2 = bm - n \in \mathbb{N}$ satisfacen

$$\begin{aligned}&m|(n + k_j), \quad j = 1, 2, \\ k_1 k_2 = (am - n)(bm - n) &= abm^2 - (a + b)mn + n^2 \\ &= abmn\left(\frac{m}{n} - \left(\frac{1}{a} + \frac{1}{b}\right)\right) + n^2 = n^2,\end{aligned}$$

como queríamos probar.

□

Lema 2.2. *La ecuación*

$$\frac{a}{n} = \frac{1}{x} + \frac{1}{y}, \tag{2.3}$$

con a y n primos entre sí, es decir, $(a,n)=1$, [1] *es soluble en enteros positivos si y solo si existen u, v tales que $uv|n$ y $a|u+v$.*

Demostración. Si $\frac{a}{n}=\frac{1}{x}+\frac{1}{y}$ y $d=(x,\ y)$, entonces $x=dx'$, $y=dy'$, con $(x',\ y')=1$ y

$$adx'y'=n(x'+y').$$

Como $(x'y',\ (x'+y'))=1$, se tiene que $x'y'|n$ y como $(a,\ n)=1$, entonces $a|(x'+y')$. Por otra parte, si existen u, v tales que $uv|n$ y $a|(u+v)$, entonces $u+v=aa'$ y

$$\frac{a}{n}=\frac{aa'}{na'}=\frac{u+v}{na'}=\frac{1}{na'/u}+\frac{1}{na'/v}.$$

□

Nota 2.1. *Si existen u, v tales que $u|n$, $v|n$ y $a|(u+v)$, entonces $(u+v)=aa'$ y*

$$\frac{a}{n}=\frac{aa'}{na'}=\frac{u+v}{na'}=\frac{1}{na'/u}+\frac{1}{na'/v}.$$

Por lo que para probar que podemos descomponer $\frac{3}{n}$ como suma de dos fracciones unitarias si y solo si n tiene un divisor que no es congruente con 1 módulo 6, basta darse cuenta de que si todos los divisores de n son congruentes con 1 módulo 6, la suma de dos de ellos no podrá ser divisible por 3. Si n tiene un divisor congruente con 2 módulo 3; sea este $3q+2$, tomando $u=1$ y $v=3q+2$, tenemos que $3q+2|n$ y $3|(3q+2+1)$.

2.2. Denominador potencia de un primo impar

Denotamos por $R(n;\ a)$ el número de pares de soluciones enteras positivas $(x,\ y)$ que satisfacen (2.3). En esta sección nos centramos en los números n tales que (2.3) no es soluble en enteros positivos x e y. Veremos que existe un conjunto de números para los que no hay solución que tiene propiedades interesantes. Para ello, denotamos a $(\mathbb{Z}/a\mathbb{Z})^*$ como los elementos de $(\mathbb{Z}/a\mathbb{Z})$ que son primos con a; $(\mathbb{Z}/a\mathbb{Z})^*$ siempre tiene $\varphi(a)$ elementos.[2] Además, definimos

$$\mathcal{E}_a=\{n\in\mathbb{N}: R(n;\ a)=0\}$$

y

$$\mathcal{E}_a^*=\{n\in\mathcal{E}_a:(n,\ a)=1\}.$$

[1] A partir de ahora nos referiremos a la notación (a,n) como el máximo común divisor entre a y n.

[2] $\varphi(m)$ es la indicatriz de Euler, que viene definida como

$$\varphi(m)=|\{k\in\mathbb{Z}:1\leq k\leq m,\ \ (k,m)=1\}|.$$

Claramente, tanto $\mathcal{E}_1$ como $\mathcal{E}_2$ están vacíos. Cuando $a \geq 3$ la estructura de $\mathcal{E}_a$ es más delicada y de gran interés.

El lema 2.2 sugiere que las soluciones de (2.3) dependen solamente de las clases de residuos de los factores de n módulo a, y por lo tanto, dependen de las clases de residuos de los factores primos de n módulo a, lo que conduce nuestro estudio a la distribución de los factores primos de n en el grupo multiplicativo $(\mathbb{Z}/a\mathbb{Z})^*$.

A continuación, estudiamos el caso donde $a = p^\gamma$ es una potencia de un primo impar en (2.3). Primero veamos un teorema sobre grupos cíclicos que nos ayudará a entender mejor la estructura de $\mathcal{E}_a$.

Teorema 2.1. *Sea G un grupo cíclico con n elementos y generado por a. Sea $b \in G$ y sea $b = a^s$. Entonces b genera el subgrupo H de G que contiene n/d elementos, donde $d = (n, s)$. Además, $\langle a^s \rangle = \langle a^t \rangle$ si y solo si $(s, n) = (t, n)$.*

Nota 2.2. *Podemos encontrar la demostración de este teorema en [8] pág. 64.*

Corolario 2.1. *Si G es un grupo cíclico finito de cardinalidad n, y H_1 y H_2 son dos subgrupos de G con igual cardinalidad, entonces $H_1 = H_2$.*

Lema 2.3. *Sea p un primo impar, $a = p^\gamma$ con $\gamma \in \mathbb{N}$, $G = (\mathbb{Z}/a\mathbb{Z})^*$ y $\varphi(a) = 2^m d$ con d impar.*[3] *Sea g una raíz primitiva módulo a. Entonces*

$$H = \{g^{2^m},\ g^{2\cdot 2^m},\ g^{3\cdot 2^m},\ \ldots,\ g^{d\cdot 2^m}\}$$

es un subgrupo de G con cardinalidad d. Además, las siguientes caracterizaciones de H son equivalentes:

1. *H es el subgrupo maximal* [4] *de G con cardinalidad impar.*
2. *H es el subgrupo maximal de G tal que $-1 \notin H$.*

Demostración. Si g es una raíz primitiva módulo a, entonces $|G| = \varphi(a)$,

$$g^{2^m d} = g^{\varphi(a)} \equiv 1 \pmod{a} \Rightarrow g^{\varphi(a)/2} \equiv -1 \pmod{a}$$

y

$$G = \{g,\ g^2,\ g^3,\ \ldots,\ g^{2^m d}\}.$$

Además, es obvio que

$$H = \{g^{2^m},\ g^{2\cdot 2^m},\ g^{3\cdot 2^m},\ \ldots,\ g^{d\cdot 2^m}\}$$

[3] $\varphi(p^\gamma) = p^{\gamma-1}(p-1)$.

[4] Un subgrupo H de un grupo G es maximal dentro de los que tienen una determinada propiedad, si los únicos subgrupos de G con dicha propiedad que lo contienen son el grupo G y el propio subgrupo H.

es un subgrupo de G con cardinalidad d.

Veamos ahora que 1. y 2. caracterizan a H.

Según el teorema de Lagrange, el cardinal de cualquier subgrupo de G divide al cardinal de G; además, por el corolario 2.1 cada subgrupo de G es único para cada cardinal. Por tanto, como d es el mayor número impar que divide a $\varphi(a)$ y $|H| = d$, entonces H es el subgrupo maximal de G con cardinalidad impar. De modo que 1. caracteriza a H.

Ahora, para probar 2. basta observar que $\{1, -1\}$ es un subgrupo de G de cardinalidad par. Por el teorema de Lagrange, si un sugrupo de G contiene a -1, su cardinalidad tiene que se par. De modo que 2. caracteriza a H.

□

Lema 2.4. *Sea $\mathbb{P}$ el conjunto de números primos. Se cumple la siguiente relación de inclusión:*

$$\{n \in \mathbb{N} : p|n,\ p \in \mathbb{P} \Rightarrow p \in H\} \subseteq \mathcal{E}_a^*.$$

Demostración. Para cualquier n en el conjunto $\{n \in \mathbb{N} : p|n,\ p \in \mathbb{P} \Rightarrow p \in H\}$, y para cualquier par de enteros positivos coprimos u y v con $uv|n$ tenemos que $u,\ v \in H$ puesto que H es un grupo. Como $-1 \notin H$, tenemos que $-v \notin H$ y, por tanto, $u \neq -v$, es decir, $a \nmid u + v$. Por último, la demostración concluye con la aplicación del lema 2.2.

□

2.3. Un problema de combinatoria

El siguiente problema que nos planteamos es hallar el número de descomposiciones de una fracción unitaria como suma de dos fracciones unitarias. A continuación, vamos a ver un teorema para calcular dicha cantidad, y una caracterización necesaria para llevar a cabo la demostración del teorema.

Teorema 2.2. *Sea $f : \mathbb{N} \to \mathbb{N}$ la función tal que para cada $n \in \mathbb{N}$, $f(n)$ denota el número de descomposiciones de la fracción unitaria $\frac{1}{n}$ como suma de dos fracciones unitarias. Entonces se cumple que $f(1) = 1$ y*

$$f\Big(\prod_{j=1}^{m} p_j^{\alpha_j}\Big) = \frac{1}{2}\left(\prod_{j=1}^{m}(2\alpha_j + 1) + 1\right),$$

con p_j, p_k primos diferentes para $j \neq k$ y $\alpha_j \in \mathbb{N}$.

Veamos una caracterización de esta función en el siguiente lema:

Lema 2.5. *$f(n)$ es igual al número de factorizaciones de n como producto de 3 factores, $n = abc$ donde $(a, b) = 1$, asumiendo que las factorizaciones abc*

y bac son las mismas, pero abc y acb son distintas [5] *para* $b \neq c$ *y* $(a, c) = 1$, *ya que generan distinta descomposición en*

$$\frac{1}{n} = \frac{1}{a(a+b)c} + \frac{1}{b(a+b)c}. \tag{2.4}$$

Demostración. Si $n = abc$, usando (2.4) obtenemos una descomposición de $\frac{1}{n}$ como la suma de dos fracciones unitarias.

A continuación, primero observamos que cada descomposición de $\frac{1}{n}$ como suma de dos fracciones unitarias tiene asociada una factorización de n, $n = abc$ con $(a,\ b) = 1$, y después probamos que si dos factorizaciones $n = a_1b_1c_1 = a_2b_2c_2$, con $(a_1,\ b_2) = 1$ y $(a_2,\ b_2) = 1$, generan la misma descomposición de $\frac{1}{n}$ como suma de dos fracciones unitarias, entonces

$$(a_1 = a_2 \wedge b_1 = b_2)$$

ó

$$(a_1 = b_2 \wedge a_2 = b_1).$$

Veamos ahora que si $\frac{1}{n} = \frac{1}{x} + \frac{1}{y}$, entonces existe una factorización de n de la forma $n = abc$, tal que $(a, b) = 1$, y $x = a(a + b)c$ e $y = a(a + b)c$. De hecho, $\frac{1}{n} = \frac{1}{x} + \frac{1}{y}$ es equivalente a $xy = (x + y)n$.

Sea $d = (x, y)$, entonces $x = da$, $y = db$, y $(a, b) = 1$. De este modo, $dab = (a + b)n$, y esto nos lleva a que $a|n$, $b|n$ y $(a + b)|d$. Por lo tanto, para $c = \frac{d}{a+b}$, $n = abc$, tenemos $x = ad = a(a + b)c$, $y = bd = b(a + b)c$, $(a, b) = 1$ y $\frac{1}{n} = \frac{1}{a(a+b)c} + \frac{1}{b(a+b)c}$.

Nos queda probar que si $n = a_1b_1c_1 = a_2b_2c_2$, $(a_1, b_1) = 1$ y $(a_2, b_2) = 1$ generan la misma descomposición según (2.4) de $\frac{1}{n}$, entonces $(a_1 = a_2 \wedge b_1 = b_2)$ ó $(a_1 = b_2 \wedge a_2 = b_1)$.

En efecto, si

$$\frac{1}{a_1(a_1 + b_1)c_1} + \frac{1}{b_1(a_1 + b_1)c_1} = \frac{1}{a_2(a_2 + b_2)c_2} + \frac{1}{b_2(a_2 + b_2)c_2}$$

son las mismas descomposiciones, entonces

$$a_1(a_1 + b_1)c_1 = a_2(a_2 + b_2)c_2 \quad \wedge \quad b_1(a_1 + b_1)c_1 = b_2(a_2 + b_2)c_2$$

ò

$$a_1(a_1 + b_1)c_1 = b_2(a_2 + b_2)c_2 \quad \wedge \quad b_1(a_1 + b_1)c_1 = a_2(a_2 + b_2)c_2.$$

Si $a_1(a_1+b_1)c_1 = a_2(a_2+b_2)c_2$, entonces $a_1^2c_1 = a_2^2c_2$. Multiplicando esta igualdad por b_1b_2, nos queda $a_1b_2 = a_2b_1$. Como $(a_1, b_1) = 1$ y $(a_2, b_2) = 1$, la anterior relación es equivalente a $a_1 = a_2$ y $b_1 = b_2$, como queríamos probar. En el otro caso se procede de forma análoga.

□

[5] Por abreviar en los siguientes resultados, nos referiremos a *abc* y *acb* como factorizaciones admisibles de n.

Ejemplo 2.1. *$f(10) = 5$, ya que para las factorizaciones admisibles de 10, $f_1 = 1 \cdot 1 \cdot 10$, $f_2 = 1 \cdot 10 \cdot 1$, $f_3 = 1 \cdot 2 \cdot 5$, $f_4 = 1 \cdot 5 \cdot 2$ y $f_5 = 2 \cdot 5 \cdot 1$, se generan las correspondientes descomposiciones en* (2.4)*:*

$$\begin{aligned}\frac{1}{10} &= \frac{1}{(1+1)10} + \frac{1}{(1+1)10} = \frac{1}{20} + \frac{1}{20} \\ &= \frac{1}{1+10} + \frac{1}{(1+10)10} = \frac{1}{11} + \frac{1}{110} \\ &= \frac{1}{(1+2)5} + \frac{1}{(1+2)2\cdot 5} = \frac{1}{15} + \frac{1}{30} \\ &= \frac{1}{(1+5)2} + \frac{1}{(1+5)2\cdot 5} = \frac{1}{12} + \frac{1}{60} \\ &= \frac{1}{(2+5)2} + \frac{1}{(2+5)5} = \frac{1}{14} + \frac{1}{35}\end{aligned}$$

Ahora ya disponemos de las herramientas necesarias para demostrar el teorema 2.2.

Demostración del teorema 2.2. En esta demostración usamos el lema 2.5 y aplicamos inducción en el número de factores primos distintos en la factorización canónica de n.

Se tiene que $f(1) = 1$, ya que existe una única factorización admisible de 1 como producto de 3 números enteros positivos.

Cuando $n = p$, con p primo, se tiene que $f(p) = 2$, porque las únicas factorizaciones admisibles posibles de p son $p = 1 \cdot 1 \cdot p$ y $p = 1 \cdot p \cdot 1$.

Si $n = p^\alpha$, $\alpha \geq 2$, suponemos que $f(p^{\alpha-1}) = \alpha$, entonces las posibles factorizaciones admisibles de n son $(1, p^\alpha, 1)$ y aquellas construidas a partir de las factorizaciones admisibles que generan (a, b, c) de $p^{\alpha-1}$, asociando p al ultimo factor c; así, el número de posibles factorizaciones admisibles de n es $f(p^\alpha) = f(p^{\alpha-1}) + 1 = \alpha + 1$.

Ahora probemos el caso general. Sea $n \geq 2$ un entero positivo con $n = \prod_{j=1}^{m} p_j^{\alpha_j}$, $m \geq 2$, y asumimos que $f(\prod_{j=2}^{m} p_j^{\alpha_j}) = \frac{1}{2}(\prod_{j=2}^{m}(2\alpha_j + 1) + 1)$. Observemos que si (a_1, b_1, c_1) y (a_2, b_2, c_2) son dos factorizaciones admisibles de $\prod_{j=2}^{m} p_j^{\alpha_j}$ y $p_1^{\alpha_1}$ respectivamente, entonces (a_1a_2, b_1b_2, c_1c_2) es una descomposición para $\prod_{j=1}^{m} p_j^{\alpha_j}$. Además, si $(a_1, b_1, c_1) \neq (1, 1, \prod_{j=2}^{m} p_j^{\alpha_j})$ y $(a_2, b_2, c_2) \neq (1, 1, p_1^{\alpha_1})$, se tiene que (a_1b_2, b_1a_2, c_1c_2) es también una factorización admisible de $\prod_{j=1}^{m} p_j^{\alpha_j}$. Estas son todas las posibles factorizaciones

admisibles de n; por lo tanto,

$$\begin{aligned} f\Big(\prod_{j=1}^{m} p_j^{\alpha_j}\Big) &= 2(f(p_1^{\alpha_1})-1)(f\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big)-1) + f\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big) + f(p_1^{\alpha_1}) - 1 \\ &= (1+2(f(p_1^{\alpha_1})-1))\left(f\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big)\right) - (f(p_1^{\alpha_1})-1) \\ &= \frac{1}{2}\left(\prod_{j=1}^{m}(2\alpha_j+1)+1+2\alpha_1\right) - \alpha_1 = \frac{1}{2}\left(\prod_{j=1}^{m}(2\alpha_j+1)+1\right) \end{aligned}$$

como queríamos probar.

□

3. La conjetura de Erdös-Straus

3.1. Números que satisfacen ESC

En esta sección vamos a ver resultados que nos ayudan a describir paramétricamente números para los que se cumple la conjetura de Erdös-Straus. Recordemos que la conjetura establece que, *dado un número entero positivo* $n \geq 2$, *existen* $x,\ y,\ z \in \mathbb{N}$ *tales que*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

Lema 3.1. *Sea* n *un número primo impar;* n *es un número de Erdös-Straus si y solo si existen* $a,\ b,\ c,\ d \in \mathbb{N}$ *tales que se cumple alguna de las siguientes condiciones:*

$$(4abc - 1)d = (a + b)n, \tag{3.1}$$

$$(4abc - 1)d = an + b. \tag{3.2}$$

Demostración. Veamos primero que ocurre si se cumple (3.1) ó (3.2). Dividiendo estas ecuaciones por $abcdn$, tenemos respectivamente

$$\frac{4}{n} = \frac{1}{abcn} + \frac{1}{bcd} + \frac{1}{acd}, \tag{3.3}$$

$$\frac{4}{n} = \frac{1}{abcn} + \frac{1}{bcd} + \frac{1}{acdn}. \tag{3.4}$$

Por otro lado, si n es un número de Erdös-Straus, es decir, existen $x,\ y,\ z \in \mathbb{N}$ tales que

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}, \tag{3.5}$$

entonces tenemos $4xyz = n(xy + yz + zx)$. Como n es primo impar, n divide a x, y ó z. Por supuesto, n no divide a los tres números a la vez, ya que tendríamos la contradicción $4 = \frac{1}{x/n} + \frac{1}{y/n} + \frac{1}{z/n}$ con x/n, y/n, z/n enteros positivos. Por lo tanto, podemos asumir sin perdida de generalidad $x = an$. Así, tenemos que (3.5) es equivalente a

$$\frac{4a - 1}{na} = \frac{1}{y} + \frac{1}{z} \Leftrightarrow \frac{1}{na} = \frac{1}{(4a - 1)y} + \frac{1}{(4a - 1)z}. \tag{3.6}$$

Como n es primo y $(4a - 1,\ a) = 1$ aplicando el lema 2.5, tenemos dos casos: $(4a - 1,\ n) = 1$ ó $(4a - 1,\ n) = n$.
En el primer caso, existen $a_1,\ a_2,\ a_3 \in \mathbb{N}$ tales que $a = a_1a_2a_3$, $(na_1,\ a_2) = 1$ y

$$(4a - 1)y = na_1(na_1 + a_2)a_3, \quad (4a - 1)z = a_2(na_1 + a_2)a_3. \tag{3.7}$$

Ya que $(na,\ 4a - 1) = (na_1a_2a_3,\ 4a - 1) = 1$, existen α y β tales que $y = \alpha na_1a_3$ y $z = \beta a_2a_3$. Aplicando esto en (3.7), tenemos $(4a - 1)\alpha =$

$(na_1 + a_2) = (4a - 1)\beta$, lo que implica que $\alpha = \beta$. Por lo tanto, $A = a_1$, $B = a_2$, $C = a_3$ y $D = \alpha$, satisfaciendo

$$(4ABC - 1)D = (nA + B).$$

Ahora consideremos el segundo caso $(4a - 1,\ n) = n$. Entonces existe j tal que

$$4a - 1 = jn. \tag{3.8}$$

Llevando esta expresión a (3.6), tenemos $\frac{1}{a} = \frac{1}{jy} + \frac{1}{jz}$. Aplicando otra vez el lema 2.5, existen $a_1,\ a_2,\ a_3 \in \mathbb{N}$ tal que $a = a_1a_2a_3$, $(a_1, a_2) = 1$ y

$$jy = a_1(a_1 + a_2)a_3, \quad jz = a_2(a_1 + a_2)a_3. \tag{3.9}$$

Como $(j,\ a) = (j,\ a_1a_2a_3) = 1$, existen α y β tales que $y = \alpha a_1a_3$ y $z = \beta a_2a_3$. Aplicando esto en (3.9), tenemos $j\alpha = a_1 + a_2 = j\beta$, lo que nos conduce a $\alpha = \beta$. Multiplicando en (3.8) por α, obtenemos $A = a_1$, $B = a_2$, $C = a_3$ y $D = \alpha$, de modo que

$$(4ABC - 1)D = (A + B)n.$$

□

Corolario 3.1. *Si n es un primo impar, las relaciones* (3.1) *y* (3.2) *son respectivamente equivalentes a* (3.3) *y* (3.4)*, donde a, b, c y d son enteros positivos.*[6]

Lema 3.2. *1. Sea n primo impar. Existen a, b, c y d enteros positivos cumpliendo* (3.1) *si y solo si existen α, β, γ y δ enteros positivos satisfaciendo*

$$\delta n = (4\alpha\beta\gamma\delta - 1) - 4\alpha^2\gamma. \tag{3.10}$$

2. Sea $n \in \mathbb{N}$, $n \geq 2$. Existen a, b, c y d enteros positivos, tales que se cumple (3.2) *si y solo si existen α, β, γ y δ enteros positivos satisfaciendo*

$$n = (4\alpha\beta\gamma - 1)\delta - 4\beta^2\gamma. \tag{3.11}$$

Demostración. 1. Sea n un primo impar cumpliendo (3.1), entonces d divide a $a + b$. Sea $e = (a + b)/d$; entonces $b = de - a$ y (3.1) se transforma en $(4acde - 1) - 4a^2c = en$. Llamando $\alpha = a$, $\beta = b$, $\gamma = c$, $\delta = e$ obtenemos (3.10). Se procede de manera análoga para demostrar que (3.10) implica (3.1).

[6] Ya que en la primera descomposición de $\frac{4}{n}$, n divide a un denominador pero es coprimo con los otros, mientras que en la segunda, solo es coprimo con uno de ellos. Estos casos son conocidos como descomposiciones de Tipo I y Tipo II de $\frac{4}{n}$ respectivalmente (Ver [6]).

2. La relación (3.2) es equivalente a que $b+d$ sea divisible por a y $n+s = 4bcd$, donde $s = (b+d)/a \Leftrightarrow d = as - b$. Llamando $\alpha = a$, $\beta = b$, $\gamma = c$, $\delta = s$ obtenemos inmediatamente (3.11). Se procede de manera análoga para demostrar que (3.11) implica (3.2).

□

Corolario 3.2. *Tomando $\beta = \gamma = 1$ en (3.11), se sigue que si $n+4$ tiene un divisor congruente con 3 módulo 4, entonces n es un número de Erdös-Straus.*

Recordemos ahora, que $(\mathbb{Z}/a\mathbb{Z})^*$ denota los elementos de $(\mathbb{Z}/a\mathbb{Z})$ que son primos con a, y que $(\mathbb{Z}/a\mathbb{Z})^*$ siempre tiene $\varphi(a)$ elementos. Cuando tomamos un representante de cada una de estas clases de equivalencia, decimos que tenemos *un sistema reducido de restos módulo a.*

En [22] Yamamoto prueba que los cuadrados perfectos no satisfacen ni (3.1) ni (3.2) con alguna restricción en los parámetros (esto lo veremos más adelante); de este modo, fijando los parámetros a, b, c, d en estas ecuaciones no podemos generar un sistema completo de residuos. El siguiente lema enfatiza esta idea sin el uso del resultado de Yamamoto.

Lema 3.3. *No podemos generar un número finito de clases de equivalencia que contengan a todos los primos de la forma $4q+5$ fijando en (3.1) o (3.2) tres de los cuatro parámetros en un subconjunto finito de $\mathbb{N}$ y el parámetro restante libre en $\mathbb{N}$.*

Demostración. Sea $S_a = \{(b,\ c,\ d) \in \mathbb{N}^3\}$ denotando el subconjunto finito de $\mathbb{N}^3$ de valores dados de $(b,\ c,\ d)$. De (3.1) o (3.2), cuando a es un valor libre en $\mathbb{N}$, cada vector fijo $(b,\ c,\ d) \in S_a$ genera una clase de residuos de números de Erdös-Straus. De forma equivalente definimos S_b, S_c y S_d. Fijamos cuatro subconjuntos S_a, S_b, S_c, S_d y probamos que existen infinitos números primos n que no pueden ser generados por (3.2) con tres de los cuatro los parámetros $(a,\ b,\ c,\ d)$ en uno de los conjuntos S_a, S_b, S_c o S_d.

Los números n generados por (3.2) con $(b,\ c,\ d) \in S_a$ son un conjunto finito ya que $a|(b+d)$. Además, observamos que en (3.11) en la demostración del lema 3.2, los números n generados por (3.2) o equivalentemente por (3.11) con $(b,\ c,\ d) \in S_c$ vienen dados por

$$n = 4(\alpha\delta - \beta)\beta\gamma - \delta = 4bcd - \frac{b+d}{a}, \quad (a,\ b,\ d) \in S_c,$$

donde $\alpha = a$, $\beta = b$, $\gamma = c$ y $\delta = (b+d)/a$. Tomando $T_c = mcm\{bd : (a,\ b,\ d) \in S_c\}$, [7] los números en $\{4T_ct + 1 : t \in \mathbb{N}\}$ (en particular los

[7] $T_c = mcm\{bd : (a,\ b,\ d) \in S_c\}$ denota el mínimo común múltiplo del producto de todos los números bd de cada terna $(a,\ b,\ d) \in S_c$.

números primos en dicho conjunto) no pueden ser generados por 3.11 con $(a,\ b,\ d) \in S_c$. Para probar esto, supongamos por contradicción que para un determinado $t \in \mathbb{N}$ existen $(a_0,\ b_0,\ d_0) \in S_c$ y $c \in \mathbb{N}$ tal que

$$4T_c t + 1 = 4b_0 c d_0 - \frac{b_0 + d_0}{a_0} \Leftrightarrow 1 = 4b_0 d_0 (c - e) - \frac{b_0 + d_0}{a_0},$$

donde $e \in \mathbb{N}$, pero eso es una contradicción ya que 1 no es un número de Erdös-Straus.

Usando los mismos argumentos y notaciones que antes, cuando $(a,\ b,\ c) \in S_d$, según la demostración de 3.11 en el lema 3.2, $(\alpha,\ \beta,\ \gamma)$ se encuentran en el subconjunto finito S_δ de $\mathbb{N}^3$, y $\delta \in \mathbb{N}$. Tomando $T_d = mcm\{(4\alpha\beta\gamma - 1) : (\alpha,\ ,\beta,\ ,\gamma) \in S_\delta\}$, los números en $\{4T_d t + 1 : t \in \mathbb{N}\}$ no pueden ser generados por 3.11 con $(a,\ b,\ c) \in S_d$. Suponemos que para $t \in \mathbb{N}$ existen $(\alpha_0,\ \beta_0,\ \gamma_0) \in S_\delta$ y $\delta \in \mathbb{N}$ tales que

$$4T_d t + 1 = (4\alpha_0\beta_0\gamma_0 - 1)\delta - 4\beta_0^2\gamma \Leftrightarrow 1 = (4\alpha_0\beta_0\gamma_0 - 1)(\delta - 4e) - 4\beta_0^2\gamma$$

para algún e, de nuevo no es posible por que 1 no es un número de Erdös-Straus. Por la simetría de b y d en 3.11 la mismo conclusión se cumple para S_b para los números $\{4T_b t + 1 : t \in \mathbb{N}\}$, donde T_b está definido como T_d. Por supuesto, todos los números

$$\{4T_b T_c T_d t + 1 : t \in \mathbb{N}\}$$

no pueden ser generados por los parámetros $(a,\ b,\ c,\ d)$ con 3 de ellos en el correspondiente conjunto S_a, S_b, S_c o S_d.

Los mismos argumentos funcionan para (3.1). Por ejemplo, uno de los parámetros a o b en (3.1) no puede tomar valores en un subconjunto infinito de enteros positivos mientras que los otros tres pertenezcan a un subconjunto finito. De hecho, observando que (3.1) es simétrico en a y b, y según la demostración de (3.10) en el lema 3.2, el número $e = (a + b)/d$ divide a $1 + 4a^2c$, así que si $(a,\ b,\ c)$ recorre un conjunto finito, el número de divisores de $1 + 4a^2c$ es finito. Además, los números n generados en (3.1) o equivalentemente en (3.10) con $(b,\ c,\ d) \in S_c$ no contienen a $\{4T_c' t + 1 : t \in \mathbb{Z}_{\geq 0}\}$ donde $T_c' = mcm\{abd : (a,\ b,\ d) \in S_c\}$. Supongamos que dado un t entonces existen $(a_0,\ b_0,\ d_0) \in S_c$ y $c \in \mathbb{N}$ tal que

$$(a_0 + b_0)(4T_c' t + 1) = (4a_0 b_0 c - 1)d_0 \Leftrightarrow (a_0 + b_0)1 = (4a_0 b_0 (c - e) - 1)d_0$$

donde $e = \frac{(a_0 + b_0)T_c' t}{a_0 b_0 d_0}$, pero otra vez, entramos en contradicción ya que 1 no es un número de Erdös-Straus. Para $(a,\ b,\ c) \in S_d$, no podemos generar los números $4T_d' t + 1$, donde $T_d' = mcm\{(4abc - 1) : (a,\ b,\ c) \in S_d\}$. Por lo tanto, las ecuaciones 3.1 y 3.2 no pueden generar los números

$$\{4T_b T_c T_d T_c' T_d' t + 1 : t \in \mathbb{N}\} \tag{3.12}$$

excepto un número finito de ellos con tres parámetros de a, b, c, d en el correspondiente conjunto S_a, S_b, S_c o S_d. □

Nota 3.1. *Usando el resultado de Yamamoto, podemos probar que las ecuaciones* (3.1) *y* (3.2) *no pueden generar todos los números* $\{4T_bT_cT_dT'_cT'_dt + n_0 : t \in \mathbb{N}\}$ *excepto un posible número finito de ellos con tres parámetros de* a, b, c, d *en el correspondiente conjunto* S_a, S_b, S_c *o* S_d, *donde* n_0 *es un residuo cuadrático módulo* $4T_bT_cT_dT'_cT'_d$.

3.2. Soluciones paramétricas

Muchos estudios prestan especial atención a las descomposiciones de Tipo II ya que las soluciones paramétricas de ESC son fácilmente obtenidas en este caso (ver [14]). A continuación, nos centraremos en las descomposiciones de Tipo I.

El siguiente lema nos permite encontrar una solución paramétrica para (3.1) en forma de descomposición de Tipo I.

Lema 3.4. *Sea* $n \in \mathbb{N}$. *Existen* a, b, c, d *enteros positivos tal que se cumple* (3.1) *si y solo si existen* x, t, λ *de modo que*

$$\begin{cases} \frac{xn+t}{\lambda} \in \mathbb{N}, \\ \frac{n+\lambda}{4xt} \in \mathbb{N}. \end{cases} \tag{3.13}$$

Demostración. Suponemos que existen enteros positivos x, t, λ, y, z tales que

$$\begin{aligned} \frac{xn+t}{\lambda} = y, \quad \frac{n+\lambda}{4xt} = z &\Leftrightarrow xn + t = y\lambda, \quad \lambda = 4zxt - n \\ &\Leftrightarrow (x+y)n = (4xyz-1)t. \end{aligned}$$

Por lo tanto, tomando $a = x$, $b = y$, $c = z$, $d = t$ tenemos $(4abc-1)d = (a+b)n$.

□

Como ya mencionábamos en la introducción, estamos interesados en los n de la forma $n = 4q+1$. Los experimentos numéricos sugieren que podemos encontrar una solución para (3.13) con $x = 1$. Como $n + \lambda \equiv 0 \pmod 4$ se tiene que $\lambda \equiv 3 \pmod 4$. De esta forma, en la búsqueda de una expresión simple de (3.13), obtenemos el polinomio $p : \mathbb{N}^3 \to \mathbb{N}$, que se define como:

$$p(\alpha,\ \beta,\ \gamma) = (\alpha+1)(4\beta+3)(4\gamma+3) - (\alpha+1) - (4\beta+3). \tag{3.14}$$

Tomando $a = (\alpha+1)$, $b = (4\beta+3)$ y $c = (4\gamma+3)$, tenemos que los números

$$n = abc - a - b \tag{3.15}$$

son números de Erdös-Straus cuando $bc \equiv 1 \pmod 4$. Además, generan la siguiente descomposición

$$\frac{4}{abc-b-c} = \frac{1}{a\frac{bc-1}{4}} + \frac{1}{a(ac-1)\frac{bc-1}{4}} + \frac{1}{(ac-1)\frac{bc-1}{4}n}.$$

Nota 3.2. *Reemplazando la condición* $bc \equiv 1 \pmod 4$ *por* $bc \equiv 1 \pmod m$, *se cumple la conjetura de Sierpiński y Schinzel para* $n = abc - a - b$.

Corolario 3.3. *Si* n *es un número de Erdös-Straus y se cumple* (3.13) *con los enteros positivos* x, t, λ, *entonces para todo* $j \in \mathbb{N}$, $N = n + 4xt\lambda j$ *es un número de Erdös-Straus. De hecho,*

$$\begin{cases} \frac{xN+t}{\lambda} = \frac{x(n+4xt\lambda j)+t}{\lambda} = \frac{xn+t}{\lambda} + 4x^2tj \in \mathbb{N} \\ \frac{N+\lambda}{4xt} = \frac{(n+4xt\lambda j)+\lambda}{4xt} = \frac{n+\lambda}{4xt} + \lambda j \in \mathbb{N}. \end{cases}$$

En particular, el conjunto de los números de Erdös-Straus es un abierto de la topología de Furstenberg (ver [15], p. 34).[8]

[8] Un conjunto N de enteros es un abierto en esta topología si para cada $n \in N$ existe una progresión aritmética $\mathcal{A}$ tal que $n \in \mathcal{A} \subseteq N$.

4. Ecuaciones en congruencias

En esta sección vamos a ver distintos resultados de ecuaciones en congruencias que nos ayudarán a probar que el conjunto $\mathcal{N}_1 = \{n \in \mathbb{N} : \exists\, \alpha,\, \beta,\, \gamma \in \mathbb{N}, n = p(\alpha,\, \beta,\, \gamma)\}$ no contiene cuadrados perfectos. En particular nos centraremos en las ecuaciones de la forma $f(x) \equiv 0 \pmod{m}$, donde f es un polinomio de grado n con $n > 1$.

4.1. Congruencias polinómicas

Ejemplo 4.1. *Resolver las ecuaciones* $x^2 \equiv 3 \pmod{7}$ *y* $x^2 \equiv 2 \pmod{7}$.

Solución. Sea $x = 7k + j$, *con* $k \in \mathbb{Z}$ *y* $j = 0, 1, 2, 3, 4, 5, 6$. *Así,* $x^2 = 49k^2 + 14kj + j^2$, *por lo que, al estudiar los distintos valores que puede tomar* j, *el correspondiente* x^2 *es congruente módulo* 7 *con* 0, 1, 4, 2, 2, 4, 1. *Por lo tanto, la ecuación en congruencias* $x^2 \equiv 3 \pmod{7}$ *no tiene solución. Por otro lado, la ecuación* $x^2 \equiv 2 \pmod{7}$ *tiene como soluciones* $x_{k_1} = 7k_1 + 3$ *y* $x_{k_2} = 7k_2 + 4$, *con* $k_1, k_2 \in \mathbb{Z}$.

Este no es un buen método para resolver estas ecuaciones. Veamos unos resultados que nos ayudarán a entender mejor este tipo de problemas. Primero de todo, observamos que la ecuación $f(x) \equiv 0 \pmod{m}$ está bien planteada en $(m\mathbb{Z})$, ya que, si un $x \in \mathbb{Z}$ es solución, también lo es toda su clase de equivalencia en $(m\mathbb{Z})$. Esto se da ya que todas las operaciones que aparecen en un polinomio están bien definidas en $(m\mathbb{Z})$, luego $f(x + km) \equiv f(x) \pmod{m}$ para todo $k \in (m\mathbb{Z})$.

Teorema 4.1. *(Lagrange, 1773). Dado un primo* p, *sea* $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ *un polinomio de grado* n *y coeficientes enteros, y con* $c_n \not\equiv 0 \pmod{p}$. *Entonces la congruencia polinómica* $f(x) \equiv 0 \pmod{p}$ *tiene a lo sumo* n *soluciones en* $(p\mathbb{Z})$

Demostración. Usaremos inducción sobre n, el grado del polinomio. Si $n = 1$, sabemos que $c_0 + c_1 x \equiv 0 \pmod{p}$, con $c_1 \not\equiv 0 \pmod{p}$, solo tiene una solución [19]. Para realizar el paso de inducción, asumimos cierta la hipótesis para polinomios de grado $n - 1$. Veamos por reducción al absurdo que también es cierta para polinomios de grado n. Supongamos que no, es decir, que un polinomio $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, con $c_n \not\equiv 0 \pmod{p}$, tiene $n + 1$ soluciones $x_0,\, x_1,\, \cdots,\, x_n$ no congruentes módulo p. Como $x^j - x_0^j = (x - x_0)(x^{j-1} + x_0 x j - 2 + x_0^2 x j - 3 + \cdots + x_0^{j-1})$, podemos poner

$$f(x) - f(x_0) = \sum_{j=0}^{n} c_j x^j - \sum_{j=0}^{n} c_j x_0^j = \sum_{j=0}^{n} c_j (x^j - x_0^j) = (x - x_0) g(x),$$

donde $g(x)$ es un polinomio de coeficientes enteros, grado $n-1$ y coeficiente director c_n. Entonces,

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p}, \quad k = 1, 2, 3, \ldots, n,$$

ya que $f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}$. Pero $x_k \not\equiv x_0 \pmod{p}$ si $k \neq 0$, y el módulo p es primo, así que, forzosamente,

$$g(x_k) \equiv 0 \pmod{p}, \quad k = 1, 2, 3, \ldots, n,$$

lo cual entra en contradicción con la hipótesis de inducción.

□

4.2. Restos cuadráticos y ley de reciprocidad cuadrática

En esta sección nos centraremos en el estudio de polinomios de la forma $f(x) = x^2 - b$. Por el teorema de Lagrange, sabemos que cuando p es un número primo, la ecuación en congruencias

$$x^2 \equiv b \pmod{p} \tag{4.1}$$

tiene, como máximo, dos soluciones. Empecemos viendo los casos más triviales. Si $p = 2$, todo es evidente, así que durante esta sección p será siempre un primo impar. También, si $b \equiv 0 \pmod{p}$ la única solución módulo p es $x = 0$. Por ello, a partir de ahora, asumiremos que $b \not\equiv 0 \pmod{p}$; o, incluso, que $0 < b < p$. Nótese además que, si x satisface (4.1), también lo hace $-x$; así que el número de soluciones de la ecuación es forzosamente 0 o 2. Cuando (4.1) tiene solución, se dice que b es *resto cuadrático* módulo p. Por el contrario, si (4.1) no tiene solución diremos que b, no es un resto cuadrático módulo p.

A partir de aquí, tenemos dos problemas que interesan resolver:

- Dado un primo p, identificar siempre si b es o no resto cuadrático módulo p.
- Dado un entero b, identificar todos los primos p tales que b es un resto cuadrático módulo p.

El siguiente teorema nos dice cuántos restos cuadráticos módulo p hay.

Teorema 4.2. *Sea p un primo impar. Entre los enteros 1, 2, ..., $p-1$, el número de restos cuadráticos módulo p es $(p-1)/2$; los otros $(p-1)/2$ números no lo son. En concreto, los restos cuadráticos son los que corresponden a las clases módulo p de los números*

$$1^2,\ 2^2,\ 3^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2. \tag{4.2}$$

Demostración. En primer lugar, comprobemos que los $(p-1)/2$ números de (4.2) son distintos módulo p. En efecto, si dos enteros x e y con $1 \leq x \leq (p-1)/2$ y $1 \leq y \leq (p-1)/2$ verifican $x^2 \equiv y^2 \pmod{p}$, entonces $(x-y)(x+y) \equiv 0 \pmod{p}$. Pero $1 \leq x+y \leq p$, y p es primo (en $(p\mathbb{Z})$ no hay divisores de 0), así que forzosamente tiene que ser $x-y \equiv 0 \pmod{p}$, luego $x = y$. Para finalizar la demostración basta darse cuenta de que, cualquiera que sea el número $x \not\equiv 0 \pmod{p}$, su cuadrado debe ser congruente módulo p con alguno de los números de (4.2), ya que $(p-k)^2 \equiv k^2 \pmod{p}$.

□

4.2.1. El símbolo de Legendre

Antes de pasar a ver más resultados, es necesario definir el denominado *símbolo de Legendre* que, para p un primo impar y $b \not\equiv 0 \pmod{p}$, se define como

$$(b|p) = \begin{cases} 1, & \text{si } b \text{ es resto cuadrático módulo } p, \\ -1, & \text{si } b \text{ no es resto cuadrático módulo } p. \end{cases} \tag{4.3}$$

Cuando $b \equiv 0 \pmod{p}$, se toma $(b|p) = 0$. Ahora, el problema de identificar si b es o no resto cuadrático módulo p se ha convertido en saber identificar $(b|p)$. Antes de pasar a ver resultados que nos proporcionen una manera directa de calcular $(b|p)$, observemos que, para p fijo, la función $(\cdot|p)$ está bien definida en $(p\mathbb{Z})$, ya que $(b|p) = (c|p)$ si $b \equiv c \pmod{p}$.

A continuación, enunciaremos el criterio de Euler, que nos proporciona una manera directa de calcular $(b|p)$; de hecho, es el que hace que la definición (4.3) sea útil.

Nota 4.1. *El valor de $b^{(p-1)/2}$ siempre es 1, -1 ó 0 módulo p: en efecto, el teorema de Euler-Fermat (o incluso aplicando el caso particular denominado teorema pequeño de Fermat* [9]*), nos asegura que, cuando $b \not\equiv 0 \pmod{p}$,*

$$(b^{\frac{(p-1)}{2}} + 1)(b^{\frac{(p-1)}{2}} - 1) = b^{(p-1)} - 1 \equiv 0 \pmod{p}, \tag{4.4}$$

y por tanto el primo p debe dividir a uno de los dos factores $b^{(p-1)/2} + 1$ o $b^{(p-1)/2} - 1$, es decir, $b^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

[9]

Teorema 4.3. *(Teorema de Euler-Fermat). Si $(a, m) = 1$, entonces $a^{\varphi(m)} \equiv \pmod{m}$.*

Corolario 4.1. *(Teorema pequeño de Fermat). Sea p un número primo y a un entero. Se cumple:*

- *Si $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.*
- *En general, sea cierta o no la hipótesis anterior $p \nmid a$, siempre se cumple $a^p \equiv a \pmod{p}$.*

Teorema 4.4. *(Criterio de Euler). Sea p un primo impar y b un entero. Entonces,* $(b|p) \equiv b^{(p-1)/2} \pmod{p}$.

Demostración. Si $b \equiv 0 \pmod{p}$ el resultado es trivial, pues $(b|p) = 0$ y $b^{(p-1)/2}$ es múltiplo de p. El caso $(b|p) = 1$ también es muy sencillo: por definición, existe un entero x, tal que $x^2 \equiv b \pmod{p}$, luego, por el teorema de Euler-Fermat (de nuevo basta usar el teorema pequeño de Fermat),

$$b^{\frac{(p-1)}{2}} \equiv (x^2)^{\frac{(p-1)}{2}} = x^{p-1} \equiv 1 \pmod{p},$$

así que efectivamente $b^{(p-1)/2} \equiv 1 = (b|p) \pmod{p}$. Finalmente, veamos el caso $(b|p) = -1$. Como el polinomio $f(x) = x^{(p-1)/2} - 1$ tiene grado $(p-1)/2$, por el teorema de Lagrange, la congruencia

$$f(x) \equiv 0 \pmod{p} \tag{4.5}$$

tiene, a lo sumo, $(p-1)/2$ soluciones. El teorema 4.2 nos asegura que hay exactamente $(p-1)/2$ restos cuadráticos módulo p, y del razonamiento usado en el caso $(b|p) = 1$ se desprende que todos ellos son soluciones de (4.5), luego los otros $(p-1)/2$ no restos cuadráticos, no pueden serlo. Así pues, un b que cumpla $(b|p) = -1$ no puede ser raíz de f, es decir, no puede cumplir $b^{(p-1)/2} \equiv 1 \pmod{p}$. Como ya hemos visto, solo existen las posibilidades $b^{(p-1)/2} \equiv 1 \pmod{p}$ o $b^{(p-1)/2} \equiv -1 \pmod{p}$, por lo que deberá ser $b^{(p-1)/2} \equiv -1 \pmod{p}$.

□

El resultado anterior nos proporciona una fórmula explícita para conocer el valor de $(b|p)$. Recordemos además, que calcular $b^{(p-1)/2}$ módulo p con p grande no es tan complicado como parece, pues se puede aplicar el algoritmo de cuadrados iterados. El criterio de Euler también permite manejar $(b|p)$ de una manera más cómoda, lo que nos ayuda a probar distintas propiedades del símbolo de Legendre. Por ejemplo, sirve para deducir que

$$(bc|p) = (b|p)(c|p) \tag{4.6}$$

para todo $b, c \in \mathbb{Z}$. Otra consecuencia inmediata es el siguiente resultado, que se obtiene sin más que tomar $b = -1$:

$$(-1|p) = (-1)^{\frac{(p-1)}{2}} = \begin{cases} 1, & si \;\; p \equiv 1 \pmod{4}, \\ -1, & si \;\; p \equiv 3 \pmod{4}. \end{cases} \tag{4.7}$$

Como paso previo a mejorar el criterio de Euler, veamos el siguiente resultado fundamental:

Teorema 4.5. *(Lema de Gauss). Sea p un primo impar y b un entero. Supongamos que $b \not\equiv 0 \pmod{p}$ y, para cada uno de los números*

$$b,\ 2b,\ 3b,\ \ldots,\ \frac{p-1}{2}b,$$

consideremos su mínimo resto positivo módulo p. Si s indica cuántos de estos restos son mayores que $p/2$, entonces $(b|p) = (-1)^s$.

Demostración. Descompongamos el conjunto $T = \{1,\ 2,\ ,\ \ldots,\ (p-1)/2\}$ en dos subconjuntos disjuntos $C = \{C_1,\ C_2,\ \ldots,\ C_r\}$ y $D = \{D_1,\ D_2,\ \ldots,\ D_s\}$ con $s = (p-1)/2 - r$ según el siguiente criterio:

- En C nos quedamos con los $t \in T$ tales que el resto de tb módulo p es menor que $p/2$.
- Mientras que en D tomamos los $t \in T$ tales que el resto de tb módulo p es mayor que $p/2$.

Así pues, $C_j b \equiv c_j \pmod{p}$ con $0 < c_j < p/2$ para $j = 1, 2, \ldots, r$ y $D_j b \equiv d_j \pmod{p}$ con $p/2 < c_j < p$ para $j = 1, 2, \ldots, s$, y todos los números

$$c_1,\ c_2,\ \ldots,\ c_r,\ p-d_1,\ p-d_2,\ \ldots,\ p-d_s \tag{4.8}$$

son positivos y menores que $p/2$. Además, son números distintos:

- Si $c_j = c_k$ tendríamos $C_j b \equiv C_k b \pmod{p}$, pero eso (dado que $b \not\equiv 0 \pmod{p}$ con p primo) implicaría que $C_j = C_k$.
- Si $p - d_j = p - d_k$ también sería $d_j = d_k$ y de nuevo obtendríamos $D_j = D_k$.
- Si $c_j = p - d_k$, deberá ser $c_j + d_k = p \equiv 0 \pmod{p}$, de donde $0 \equiv c_j + d_k \equiv (C_j + D_k)b \pmod{p}$, y por tanto también $C_j + D_k \equiv 0 \pmod{p}$; pero eso es imposible ya que $C_j + D_k$ son números positivos menores que $p/2$.

Así pues, los números listados en (4.8) son todos los enteros entre 1 y $(p-1)/2$ (ambos incluidos), y su producto es $((p-1)/2)!$. Pero también

$$C_1 C_2 \cdots C_r D_1 D_2 \cdots D_s = 1 \cdot 2 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!.$$

En consecuencia, módulo p se cumple

$$\begin{aligned} b^{\frac{(p-1)}{2}} \left(\frac{p-1}{2}\right)! &= (C_1 b)(C_2 b)\cdots(C_r b)(D_1 b)(D_2 b)\cdots(D_s b) \\ &\equiv c_1 c_2 \cdots c_r d_1 d_2 \cdots d_s \\ &\equiv (-1)^s c_1 c_2 \cdots c_r (p-d_1)(p-d_2)\cdots(p-d_s) \\ &\equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p}. \end{aligned}$$

Al ser p primo, podemos simplificar $((p-1)/2)!$ módulo p, y por tanto $b^{(p-1)/2} \equiv (-1)^s \pmod{p}$. Aplicando el criterio de Euler, $(b|p) \equiv b^{(p-1)/2} \pmod{p}$, obtenemos $(b|p) \equiv (-1)^s \pmod{p}$, y de aquí, $(b|p) = (-1)^s$. $\square$

En la práctica, no es necesario conocer el valor exacto de s para usarlo en $(-1)^s$, sino únicamente su paridad. Para dar solución a esto, enunciamos el siguiente teorema:

Teorema 4.6. *El número s que aparece en el lema de Gauss cumple*

$$s \equiv \sum_{t=1}^{\frac{(p-1)}{2}} \left\lfloor \frac{tb}{p} \right\rfloor + (b-1)\frac{p^2-1}{2} \pmod{2}, \tag{4.9}$$

donde $\lfloor \cdot \rfloor$ denota la parte entera de un número real.

Demostración. Siguiendo con la notación que teníamos en la demostración del teorema anterior, escribamos las relaciones $C_j b \equiv c_j \pmod{p}$ con $0 < c_j < p/2$ para $j = 1,\ 2,\ ,\ \ldots,\ r$ y $D_j b \equiv d_j \pmod{p}$ con $p/2 < d_j < p$ para $j = 1,\ 2,\ ,\ \ldots,\ s$, como

$$C_j b = \left\lfloor \frac{C_j b}{p} \right\rfloor p + c_j \quad y \quad D_j b = \left\lfloor \frac{DC_j b}{p} \right\rfloor p + d_j.$$

Sean asimismo

$$m = \left\lfloor \frac{b}{p} \right\rfloor + \left\lfloor \frac{2b}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2}\frac{b}{p} \right\rfloor,$$

$$c = c_1 + c_2 + \cdots + c_r \quad y \quad d = d_1 + d_2 + \cdots + d_s.$$

Sumando estas expresiones, es claro que

$$(C_1 + C_2 + \cdots + C_r + D_1 + D_2 + \cdots + D_s)b = pm + c + d. \tag{4.10}$$

Recordemos que la suma de una progresión aritmética $x_1 + x_2 + \cdots + x_k$ es $(x_k + x_1)k/2$. Entonces,

$$\begin{aligned} C_1 + C_2 + \cdots + C_r + D_1 + D_2 + \cdots + D_s \\ = 1 + 2 + \cdots + \frac{p-1}{2} = \frac{\frac{p-1}{2}+1}{2}\frac{p-1}{2} = \frac{p+1}{4}\frac{p-1}{2} = \frac{p^2-1}{8} \end{aligned} \tag{4.11}$$

y (4.10) queda

$$\frac{p^2-1}{8}b = pm + c + d. \tag{4.12}$$

Por otra parte, tengamos en cuenta que los números listados en (4.8) son todos los enteros entre 1 y $(p-1)/2$ (ambos incluidos), con lo cual la suma es

$$\begin{aligned}\frac{p^2-1}{8} &= 1+2+\cdots+\frac{p-1}{2}\\ &= c_1+c_2+\cdots+c_r+(p-d_1)+(p-d_2)+\cdots+(p-d_s)\\ &= c+ps-d.\end{aligned} \tag{4.13}$$

Restando (4.12) y (4.13) llegamos a

$$(b-1)\frac{p^2-1}{8} = mp-sp+2d,$$

luego

$$(b-1)\frac{p^2-1}{8} - mp \equiv -sp \pmod 2.$$

Ahora, sin más que fijarse en que $p \equiv -1 \pmod 2$, obtenemos (4.9).

□

En particular, si en (4.9) tomamos $b=2$, todos los sumandos $\left\lfloor \frac{tb}{p} \right\rfloor$ se anulan. De ahí se sigue que

$$(2|p) = (-1)^{\frac{(p^2-1)}{8}} = \begin{cases} 1, & si\ p \equiv \pm 1 \pmod 8,\\ -1, & si\ p \equiv \pm 3 \pmod 8.\end{cases} \tag{4.14}$$

Finalizaremos este apartado recalcando que, como consecuencia de (4.6), el símbolo de Legendre $(\cdot|p)$ para p un primo fijo está completamente determinado por sus valores en -1, 2 y los primos impares. En concreto, si b es un entero no divisible por p y escribimos $b = \pm 2^{c_0} q_1^{c_1} q_2^{c_2} \cdots q_k^{c_k}$ con q_j primos distintos entre sí y distintos de p, entonces

$$(b|p) = (\pm 1|p)(2|p)^{c_0}(q_1|p)^{c_1}(q_2|p)^{c_2}\cdots(q_k|p)^{c_k}.$$

Además, los valores de $(\pm 1|p)$ y $(2|p)$ vienen dados en (4.7) y (4.14). Asumiendo que podemos encontrar la descomposición en factores primos,[10] calcular $(b|p)$ se reduce a conocer $(q|p)$ con q primo impar.

[10] No nos referimos a que tal descomposición exista- eso es el teorema fundamental de la aritmética-, sino a que podamos hallarla de manera efectiva, lo cual no siempre es fácil si los números involucrados son «grandes».

4.2.2. Ley de reciprocidad cuadrática

Ya hemos resuelto el primero de los dos problemas que planteábamos al principio de la sección. La solución del segundo problema es más complicada, y depende de un resultado notable, conocido como ley de reciprocidad cuadrática. Dados p y q primos impares distintos, que q sea un resto cuadrático módulo p está relacionado con que p sea un resto cuadrático módulo q. A continuación vamos a enunciar la ley de reciprocidad cuadrática mediante la formulación dada por Legendre, junto con una demostración dada por el joven matemático Ferdinand Gotthold Max Eisenstein en 1844, que reduce la prueba a contar los puntos de coordenadas enteras de dos triángulos, y que es una simplificación de una de las originales de Gauss:

Teorema 4.7. *(Ley de reciprocidad cuadrática). Si p y q son primos impares, se cumple*

$$(p|q)(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}. \tag{4.15}$$

Demostración. Tomemos $b = q$ en el teorema 4.6. Entonces, el lema de Gauss queda

$$(q|p) = (-1)^s \ \ con \ \ s = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2}\frac{q}{p} \right\rfloor.$$

Además, intercambiando los papeles de p y q tendremos

$$(p|q) = (-1)^{s'} \ \ con \ \ s' = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{q-1}{2}\frac{p}{q} \right\rfloor.$$

Por tanto, $(p|q)(q|p) = (-1)^{s+s'}$ y la demostración estará completa si vemos que

$$s + s' = \frac{p-1}{2}\frac{q-1}{2}.$$

Para comprobarlo, vamos a ayudarnos de la figura 3.

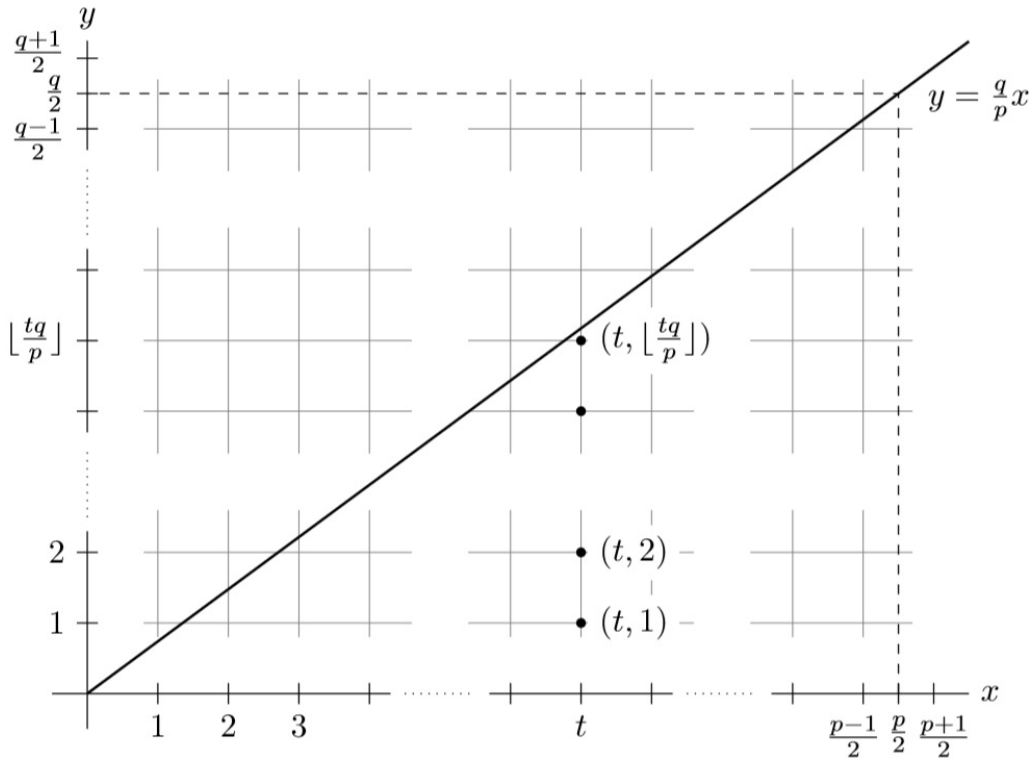


Figura 3: Puntos de coordenadas enteras del rectángulo $1 \leq x \leq p/2$, $1 \leq y \leq q/2$. Aparecen marcados los puntos $(t,\, n)$ con $n = 1,\, 2,\, \ldots,\, \lfloor tq/p \rfloor$.

Por una parte, es claro que en el rectángulo $1 \leq x \leq p/2$, $1 \leq y \leq q/2$ hay $\frac{p-1}{2}\frac{q-1}{2}$ puntos de coordenadas enteras. Por la otra, vamos a ver que por debajo de la recta $y = \frac{q}{p}x$ hay s de tales puntos; y, por encima de ella, s' (no puede haber ninguno sobre la recta ya que $(p, q) = 1$). En la región del rectángulo situada por debajo de esa recta, detengámonos en la recta vertical $x = t$ (con t un entero entre 1 y $p/2$), cuya intersección con $y = \frac{q}{p}x$ es $(t,\, tq/p)$. Sobre esa recta vertical están los puntos $(t,\, 1)$, $(t,\, 2)$, $\ldots$ hasta $(t,\, \lfloor tq/p \rfloor)$; es decir, hay $\lfloor tq/p \rfloor$ puntos de coordenadas enteras. Contando los puntos de todas las rectas verticales, en esta región hay

$$\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{tq}{p} \right\rfloor + \cdots + \left\lfloor \frac{p-1}{2}\frac{q}{p} \right\rfloor = s$$

puntos. Finalmente, intercambiando los paples de p y q se obtiene que en la región del rectángulo por encima de la recta $y = \frac{q}{p}x$ hay s' puntos.

□

Si p y q son primos impares la fórmula (4.15) es una forma resumida de decir lo siguiente:

- Si p y q son congruentes con 3 módulo 4, entonces p es resto cuadrático módulo q si y solo si q no es resto cuadrático módulo p.
- En otro caso, p es resto cuadrático módulo q si y solo si q es resto cuadrático módulo p.

Veamos a continuación unos ejemplos donde aplicamos la ley de reciprocidad cuadrática para calcular el símbolo de Legendre con poco trabajo:

Ejemplo 4.2. *Calcular* $(33|97)$.

Solución. Como 97 es primo pero 33 no, descomponemos $33 = 11 \cdot 3$. *Entonces aplicando las propiedades del símbolo de Legendre (entre ellas, la ley de reciprocidad cuadrática, teniendo en cuenta que* $97 \equiv 1 \pmod 4$ *y* $11 \equiv 3 \pmod 4$*), obtenemos*

$$(33|97) = (3|97)(11|97) = (97|3)(97|11) = (1|3)(9|11) = 1 \cdot 1 = 1.$$

La ley de reciprocidad cuadrática da, además, una respuesta parcial al segundo problema planteado al principio de la sección. En efecto, si solo consideramos los b que sean primos (es decir, $b = q$, en la ley de reciprocidad cuadrática), la fórmula (4.15) representa una especie de dualidad entre el primer problema y el segundo. Conociendo $(p|q)$, es inmediato calcular $(q|p)$

Ejemplo 4.3. *Identificar todos los primos p (impares) tales que 5 es resto cuadrático módulo p.*

Solución. Como $5 \equiv 1 \pmod 4$*, la ley de reciprocidad cuadrática siempre da* $(p|5)(5|p) = 1$*, y por tanto* $(5|p) = (p|5)$ *para cualquier primo impar p. De aquí que*

$$(5|p) = (p|5) = \begin{cases} 1, & \text{si } p \equiv 1 \text{ o } 4 \pmod 5, \\ -1, & \text{si } p \equiv 2 \text{ o } 3 \pmod 5. \end{cases}$$

Así pues, 5 es resto cuadrático módulo p si y solo si $p \equiv 1 \text{ o } 4 \pmod 5$.

4.3. El símbolo de Jacobi

El símbolo de Jacobi es una generalización del símbolo de Legendre. Vamos a explicar en que consiste esta generalización. Si $P > 1$ es un entero impar cuya descomposición en factores primos distintos es $P = \prod_{j=1}^{s} p_j^{a_j}$, y b es un número entero, el *símbolo de Jacobi* es, por definición,

$$(b|P) = \prod_{j=1}^{s} (b|p_j)^{a_j}, \tag{4.16}$$

donde $(b|p_j)$ es el símbolo de Legendre. Si $P = 1$, se toma $(b|P) = 1$. Es claro que $(b|P)$ solo puede valer 1, -1 o 0 (esto último si y solo si $(b, P) > 1$).

Son inmediatas de comprobar las siguientes propiedades, en las que P y Q denotan enteros positivos impares, y b y c enteros arbitrarios:

- $(b|P) = (c|P)$ si $b \equiv c \pmod{P}$,
- $(bc|P) = (b|P)(c|P)$,
- $(b|PQ) = (b|P)(b|Q)$,
- $(b^2|P) = 1)$ si $(b, P) = 1$.

También son ciertas las siguientes fórmulas, análogas a las del símbolo de Legendre:

Proposición 4.1. *Si P es un entero positivo impar, entonces*

$$(-1|P) = (-1)^{(P-1)/2}, \tag{4.17}$$

$$(2|P) = (-1)^{(P^2-1)/8}. \tag{4.18}$$

Demostración. Escribamos $P = p_1 p_2 \cdots p_s$, donde los factores primos p_j no son necesariamente distintos, como

$$P = \prod_{j=1}^{s}(1 + (p_j - 1)) = 1 + \sum_{j=1}^{s}(p_j - 1) + \sum_{j \neq k}(p_j - 1)(p_k - 1) + \cdots .$$

Cada factor $p_j - 1$ es par, así que

$$P \equiv 1 + \sum_{j=1}^{s}(p_j - 1) \pmod{4},$$

y de aquí

$$\frac{1}{2}(P - 1) \equiv \sum_{j=1} \frac{1}{2}(p_j - 1) \pmod{2}. \tag{4.19}$$

Con esto, aplicando (4.7) a cada factor se sigue (4.17):

$$(-1|P) = \prod_{j=1}^{s}(-1|p_j) = \prod_{j=1}^{s}(-1)^{(p_j-1)/2} = (-1)^{(P-1)/2}.$$

Para probar (4.18) escribamos

$$P^2 = \prod_{j=1}^{s} p_j^2 = \prod_{j=1}^{s}(1 + (p_j^2 - 1)) = 1 + \sum_{j=1}^{s}(p_j^2 - 1) + \sum_{j \neq k}(p_j^2 - 1)(p_k^2 - 1) + \cdots .$$

Como cada p_j es impar, $p_j^2 - 1 = (p_j - 1)(p_j + 1)$ es múltiplo de 8, así que

$$P^2 \equiv 1 + \sum_{j=1}^{s} (p_j^2 - 1) \pmod{64},$$

y por tanto

$$\frac{1}{8}(P^2 - 1) \equiv \sum_{j=1}^{s} \frac{1}{8}(p_j^2 - 1) \pmod{8};$$

en particular, también

$$\frac{1}{8}(P^2 - 1) \equiv \sum_{j=1}^{s} \frac{1}{8}(p_j^2 - 1) \pmod{2}.$$

Con esto, de (4.14) obtenemos

$$(2|P) = \prod_{j=1}^{s} (2|p_j) = \prod_{j=1}^{s} (-1)^{(p_j^2-1)/8} = (-1)^{(P^2-1)/8}.$$

□

Con el símbolo de Jacobi no es cierto que $(b|P)$ vale -1 o 1 en función si la ecuación $x^2 \equiv b \pmod{P}$ tiene solución o no. Veamos a continuación la ley de reciprocidad cuadrática extendida a los símbolos de Jacobi.

Teorema 4.8. *(Ley de reciprocidad cuadrática para símbolos de Jacobi). Si P y Q son enteros positivos impares con $(P,\ Q) = 1$, se cumple*

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}$$

Demostración. Representemos las descomposiciones de P y Q en factores primos como $P = p_1 p_2 \dots p_s$ y $Q = q_1 q_2 \dots q_t$ (nótese que, por ser $(P,\ Q) = 1$, se cumplirá $p_j \neq q_k$ para todo j, k). Aplicando la definición de símbolo de Jacobi, la propiedad $(bc|P) = (b|P)(c|P)$, y la ley de reciprocidad cuadrática para símbolos de Legendre, tenemos

$$(P|Q)(Q|P) = \prod_{j=1}^{s} \prod_{k=1}^{t} (p_j|q_k)(q_k|p_j) = (-1)^r$$

con

$$r = \sum_{j=1}^{s} \sum_{k=1}^{t} \frac{(p_j - 1)(q_k - 1)}{4}.$$

Escribamos este r como

$$r = \sum_{j=1}^{s}\sum_{k=1}^{t}\frac{1}{2}(p_j-1)\frac{1}{2}(q_k-1) = \left(\sum_{j=1}^{s}\frac{1}{2}(p_j-1)\right)\left(\sum_{k=1}^{t}\frac{1}{2}(q_k-1)\right)$$

y tengamos en cuenta que, tal como hemos visto en (4.19) (con su análogo para Q)

$$\frac{1}{2}(P-1) \equiv \sum_{j=1}^{s}\frac{1}{2}(p_j-1) \pmod 2, \qquad \frac{1}{2}(Q-1) \equiv \sum_{k=1}^{t}\frac{1}{2}(q_j-1) \pmod 2.$$

En consecuencia,

$$r \equiv \frac{1}{2}(P-1)\frac{1}{2}(Q-1) \pmod 2,$$

como queríamos probar.

□

Acabemos esta sección mencionando una extensión del símbolo de Jacobi: el símbolo de Kronecker, en el que, se llega a definir $(b|P)$ cuando P es un entero que puede ser par. Este símbolo cumple $(n|m) = 0$ para $(n,\ m) \geq 2$. A pesar de que las propiedades de este símbolo ya no son tan útiles, usaremos la siguiente propiedad para probar una caracterización de $\mathcal{N}_1$ en la siguiente sección:

$$\text{Si } (P,b) = 1 \text{ y } P \equiv -Q \pmod b \ (b|P) = (b|Q)$$

Nota 4.2. *Podemos encontrar una demostración detallada de esta propiedad en [11] pág. 305.*

4.4. $\mathcal{N}_1$ no contiene cuadrados perfectos

En este apartado probaremos que $\mathcal{N}_1 = \{n \in \mathbb{N} : \exists\, \alpha,\ \beta,\ \gamma \in \mathbb{N}, n = p(\alpha,\ \beta,\ \gamma)\}$ no incluye a los cuadrados perfectos. Para ello usaremos el símbolo de Jacobi visto en la sección anterior. En [22], Yamamoto observa que los números n que satisfacen $(4abc-1)d = (a+b)n$ para ciertos a, b, c, d con $(n,\ abd) = 1$, no son cuadrados perfectos. No obstante, pasa por alto la condición de que $(d,n) = 1$, ya que si $(4abc-1)d = (a+b)n$, entonces $(4abc-1)d' = (a+b)n^2$ con $d' = dn$. También observa la simetría de a y b en $(4abc-1)d = (a+b)n$, y prueba usando el símbolo de Kronecker que $(n|4ad) = -1$. Nuestra clase $\mathcal{N}_1$ contiene a los números n que no están incluidos en la clase de Yamamoto. Por ejemplo, en el caso de $n = 2009$,

donde $a = 1$, $b = 293$, $c = 12$ y $d = 42$, mientras que $\alpha + 1 = 42$, $4\beta + 3 = 7$ y $4\gamma + 3 = 7$. De hecho, tenemos

$$\begin{aligned} 2009 &= 42 \cdot 7 \cdot 7 - 42 - 7, \\ 2009(1 + 293) &= (4 \cdot 1 \cdot 293 - 1)42, \\ (2009,\ 293 \cdot 42) &= 7. \end{aligned}$$

Lema 4.1. *$\mathcal{N}_1$ no contiene cuadrados perfectos.*

Demostración. sea $n \in \mathcal{N}_1$. Existen tres enteros positivos α, β, γ tales que

$$n + (4\beta + 3) = (\alpha + 1)((4\beta + 3)(4\gamma + 3) - 1) \stackrel{\text{def}}{=} (\alpha + 1)\tau,$$

donde $\tau = (4\beta + 3)(4\gamma + 3) - 1$. Ya que $(4\beta + 3, \tau) = 1$, también tenemos $(n,\ \tau) = 1$ y $(n + \tau,\ \tau) = 1$. Usando la ley de reciprocidad para el símbolo de Jacobi, obtenemos

$$(n|n + \tau)(n + \tau|n) = (-1)^{\frac{n-1}{2}\frac{n+\tau-1}{2}} = 1. \tag{4.20}$$

Aquí hemos usado que $n \equiv 1 \pmod 4$. Como $n + \tau \equiv \tau \pmod n$, tenemos $(n + \tau|n) = (\tau|n)$. Teniendo en cuenta que $n \equiv -(4\beta + 3) \pmod \tau$ y las propiedades del símbolo de Jacobi, llegamos a $(\tau|n) = (\tau|4\beta + 3)$. También, como $\tau \equiv -1 \pmod{4\beta + 3}$ y usando que si $n \equiv 3 \pmod 4$, $(-1|n) = -1$, obtenemos $(\tau|4\beta + 3) = (-1|4\beta + 3) = -1$. Por lo tanto, de (4.20) llegamos a $(n|n + \tau) = -1$, lo cual implica que n no es un cuadrado perfecto.

□

Como $4(n^2 + n - 1) + 5 = (2n + 1)^2$, y $4q(\alpha,\ \beta,\ \gamma) + 5 = p(\alpha,\ \beta,\ \gamma)$, donde $p(\alpha,\ \beta,\ \gamma)$ y $q(\alpha,\ \beta,\ \gamma)$ están dados en (3.14) y (5.2) respectivamente. El lema 4.1 nos da inmediatamente el siguiente resultado:

Corolario 4.2. *El número $n^2 + n + \beta + 1$, con n, $\beta \in \mathbb{N}$, no tiene divisores congruentes con $3\beta + 2$ módulo $4\beta + 3$.*

5. Propiedades de los números de Erdös-Straus

5.1. Números consecutivos

En esta sección veremos un teorema importante sobre *números consecutivos* que cumplen la conjetura de Erdös-Straus, y enunciaremos los resultados necesarios para llevar a cabo su demostración. Más adelante, veremos como probar que el conjunto

$$\mathcal{N}_1 = \{n \in \mathbb{N} : \exists\, \alpha,\ \beta,\ \gamma \in \mathbb{N}, n = p(\alpha,\ \beta,\ \gamma)\}$$

contiene a los primos de la forma $n = 4q + 5$, $q \in \mathbb{N}$, hasta cierto N.

Teorema 5.1. *Existe una sucesión de números consecutivos tan larga como se quiera de modo que dichos números satisfacen la conjetura de Erdös-Straus.*

Nota 5.1. *Los valores*

$$n = p(\alpha,\ \beta,\ \gamma) = (\alpha+1)(4\beta+3)(4\gamma+3) - (\alpha+1) - (4\beta+3) \tag{5.1}$$

satisfacen (3.8) *con* $x = 1$, $t = \alpha + 1$, *y* $4\beta + 3$.

La relación paramétrica (5.1) es útil para reescribir p de la forma $p = 4q + 5$:

$$p(\alpha,\ \beta,\ \gamma) = 4((4\beta+3)\gamma + (3\beta+2))(\alpha+1) - (\beta+2)) + 5 = 4q(\alpha,\ \beta,\ \gamma) + 5$$

donde

$$q(\alpha,\ \beta,\ \gamma) = ((4\beta+3)\gamma + (3\beta+2))(\alpha+1) - (\beta+2).$$

Lema 5.1. *Si existen* $\alpha,\ \beta,\ \gamma \in \mathbb{N}$ *tales que*

$$q = q(\alpha,\ \beta,\ \gamma) = ((4\beta+3)\gamma + (3\beta+2))(\alpha+1) - (\beta+2) \tag{5.2}$$

entonces la Conjetura de Erdös-Straus se cumple para $p = 4q + 5$.

Ahora ya tenemos las herramientas necesarias para, usando el *teorema chino del resto* y el lema anterior, probar el teorema 5.1. En realidad, lo que probamos es que existe una secuencia arbitraria de clases de residuos consecutivos tales que $\frac{4}{n}$ tiene una descomposición de Tipo I para todo n en esa clase de residuos.

Demostración del teorema 5.1. Por su puesto, para demostrar el teorema 5.1 basta considerar números *"consecutivos"* de la forma $n \equiv 1$ (mód 4). Sea N un entero positivo arbitrario y sea A el subconjunto de $\mathbb{Z}$ que contiene los primeros N enteros no negativos; es decir, $A = \{0,\ 1,\ 2,\ \ldots,\ N-1\}$. Si

$\{\beta_1,\ \beta_2\} \subset A$, entonces el máximo común divisor de $4\beta_1 + 3$ y $4\beta_2 + 3$, es un número impar y

$$(4\beta_1 + 3,\ 4\beta_2 + 3)|(4\beta_1 + 3 - (4\beta_2 + 3)) = 4(\beta_1 - \beta_2)$$

$$\Longrightarrow (4\beta_1 + 3,\ 4\beta_2 + 3)|4(\beta_1 - \beta_2) = 3\beta_1 + 2 - (3\beta_2 + 2).$$

Así, por el Teorema Chino de los restos, existe un número natural T tal que

$$T \equiv 3\beta_j + 2 \pmod{4\beta_j + 3}, \quad \forall \beta_j \in A,$$

i.e., existen enteros positivos γ_j tales que

$$T = (4\beta_j + 3)\gamma_j + 3\beta_j + 2 \quad \forall \beta_j \in A.$$

De acuerdo con el lema 5.1 todo $n = 4q + 5$ con q en la clase de residuo consecutiva $-(\beta_j + 2) \pmod{T}$, $\beta_j \in A$, satisface la Conjetura de Erdös-Straus. □

Nota 5.2. *Además, también podemos probar que existe una secuencia arbitraria de números consecutivos n tal que* $\frac{4}{n}$ *tiene una descomposición de Tipo II. Sea A un conjunto de números naturales que contiene números consecutivos, para cada* $a \in A$*, elegimos los números naturales* $\beta(a)$ *y* $\gamma(a)$ *de manera que* $a = \beta(a)^2\gamma(a)$ *(tal representación es única tomando* $\gamma(a)$ *libre de cuadrados). Elegimos T como el mínimo común múltiplo de* $(4\beta(a)\gamma(a)-1)$*, cuando a toma valores en A; i.e.*

$$T = mcm\{(4\beta(a)\gamma(a) - 1) : a \in A\},\ y\ \delta = \begin{cases} 1, & si\ T \equiv 1 \pmod 4, \\ 3, & si\ T \equiv -1 \pmod 4, \end{cases}$$

entonces, usando (3.11) *en el lema 3.2, llegamos a que todas las fracciones* $\frac{4}{T\delta - 4a}$*, con* $a \in A$*, tienen descomposición de Tipo II.*

5.2. Conjetura-q

Hemos visto que basta comprobar la conjetura de Erdös-Straus para los números de la forma $n = 4q + 5$. Además, ya sabemos que el polinomio $p(x,\ y,\ z)$ no recorre los cuadrados perfectos; incluso la sección anterior nos hace pensar que basta estudiar el polinomio $q(x,\ y,\ z)$. Para completar el recorrido de todos los naturales debemos incluir expresiones asociadas a números compuestos, ya que muchos de los razonamientos que llevaron a considerar el polinomio $p(x,\ y,\ z)$ asumían que los números a considerar eran números primos. Así llegamos al siguiente resultado:

Lema 5.2. *La conjetura de Erdös-Straus se cumple si y solo si para cada* $q \in \mathbb{N}$ *existen* $x,\ y,\ z \in \mathbb{N}$ *de manera que se cumple una de las siguientes relaciones*

$$q = 1 + 3x + 3y + 4xy, \tag{5.3}$$

$$q = 5 + 5x + 5y + 4xy, \tag{5.4}$$

$$q = q(x,\ y,\ z). \tag{5.5}$$

Recordemos que $q(x,\ y,\ z)$ *está definido como:*

$$q(x,\ y,\ z) = ((4y + 3)z + (3y + 2))(x + 1) - (y + 2). \tag{5.6}$$

Demostración. Como

$$q = 1 + 3x + 3y + 4xy \Leftrightarrow 4q + 5 = (4x + 3)(4y + 3),$$

$$q = 5 + 5x + 5y + 4xy \Leftrightarrow 4q + 5 = (4(x + 1) + 1)(4(y + 1) + 1),$$

si $4q+5$ es un número compuesto, entonces q satisface (5.3) o (5.4) También hemos comprobado que para $q(x,\ y,\ z)$ definido como en (5.6),

$$q = q(x,\ y,\ z) = \frac{p(x,\ y,\ z) - 5}{4}.$$

Por lo tanto, si $\forall q \in \mathbb{N}$ se cumple (5.3), (5.4) o (5.5), el valor de q para todos los números primos de la forma $4q + 5$ está en $\mathcal{N}_1$ y la demostración concluye al aplicar el lema 5.1.

□

5.3. Densidad uno

Resulta interesante comprobar que la densidad de los números para los que se cumple la conjetura de Erdös-Straus es uno; para ello, veamos que la densidad de los números para los que la conjetura posiblemente no es cierta es cero. Definamos primero la noción de densidad:

Definición 5.1. *Sea* $A \subset \mathbb{N}$, $\forall N \in \mathbb{N}$ *tenemos el conjunto* $A(N) = \{n \in A : n \leq N\}$. *Suponemos que*

$$\lim \frac{|A(N)|}{N} = L.$$

Entonces decimos que el conjunto $N(A)$ *tiene densidad* L.

Teorema 5.2. *El conjunto de los números que cumplen la conjetura de Erdös-Straus tiene densidad uno.*

Para probar esto, vamos a comprobar que podemos aislar los números para los que la conjetura posiblemente no se cumple, en un conjunto de densidad cero. A continuación, vamos a ver un lema que nos ayuda en la demostración del teorema 5.3, donde caracterizamos los números que pueden expresarse como suma de dos cuadrados.

Lema 5.3. *1. Si p es un número primo y $p \equiv 1 \pmod 4$, entonces existen a y b enteros positivos tales que $p = a^2 + b^2$.*

2. Sea q un factor de $a^2 + b^2$. Si $q \equiv 3 \pmod 4$ entonces $q|a$ y $q|b$.

Nota 5.3. *La demostración de este lema la podemos encontrar en [15], págs. 54–55.*

Teorema 5.3. *(Fermat) Sea n con descomposición canónica*

$$n = 2^\alpha \prod_{p \equiv 1(4)} p^\beta \prod_{p \equiv 3(4)} q^\gamma.$$

Entonces n puede expresarse como suma de dos cuadrados de números enteros si y solo si todos los exponentes γ son pares.

Demostración. La identidad

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bc)^2$$

se cumple para cualesquiera números reales. En particular, esto implica que si m y n son ambos suma de dos cuadrados de números enteros, entonces mn también lo es. El número primo $2 = 1^2 + 1^2$ es suma de dos cuadrados, y cada número primo tal que $p \equiv 1 \pmod 4$, es suma de dos cuadrados. Si q es un número primo, $q \equiv 3 \pmod 4$, entonces $q^2 = q^2 + 0^2$ es una suma de dos cuadrados. Por lo tanto, cualquier número que puede ser expresado como producto de potencias de 2, p y q^2 es una suma de dos cuadrados. Por el otro lado, supongamos que n es suma de dos cuadrados, $n = a^2 + b^2$. Si q es un número primo, $q \equiv 3 \pmod 4$, con $\gamma > 0$, entonces $q|n$ y por el lema anterior, tenemos que $q|a$ y $q|b$, lo cual implica que $q^2|n$. Esto es, $\gamma \geq 2$, y podemos escribir $\frac{n}{q^2} = (a/q)^2 + (b/q)^2$. Aplicando el mismo argumento a n/q^2 resulta que si $\gamma > 2$, $\gamma \geq 4$ y $q^2|a$ y $q^2|b$. Como este proceso debe acabar, concluimos que γ debe ser par y además, $q^{\gamma/2}|a$ y $q^{\gamma/2}|b$.

□

Veamos ahora, un teorema demostrado por Landau [12] en 1908, que caracteriza la cardinalidad del conjunto de los números que son suma de dos cuadrados:

Teorema 5.4. *(Landau). Sea* $N_2(X) = \{n \in \mathbb{N} : n \leq X,\ n$ *es suma de dos cuadrados* $\}$. *Cuando* $X \to \infty$

$$|N_2(X)| \sim K \frac{X}{\sqrt{\log(X)}},$$

con

$$K = \frac{1}{\sqrt{2}} \prod_{\substack{p \equiv 3 \\ (\text{mód } 4)}} \left(1 - \frac{1}{p^2}\right)^{-1/2}$$

$$= 0{,}764223653589220662990698731250092328116790541393409514 72\ldots.[5]$$

Demostración. Esta demostración es interesante porque utiliza los mismos métodos que la del teorema sobre distribución de los números primos, pero en este caso la función tiene una singularidad algebraica. A continuación daremos unas ideas básicas de esta demostración. Para ver la demostración completa consultar [13], aunque aquí seguimos las ideas expuestas en [10] ya que resultan más sencillas de comprender.

Denotamos los primos de la forma $4m + 1$ y $4m + 3$ por q y r respectivamente.

Definimos

$$b_n = \begin{cases} 1, & \text{si } n \text{ es un cuadrado o suma de dos cuadrados,} \\ 0, & \text{en otro caso.} \end{cases}$$

Consideremos la función de Dirichlet f asociada a $\{b_n\}$[11],

$$f(s) := \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \frac{1}{1 - 2^{-s}} \prod_q \frac{1}{1 - q^{-s}} \prod_r \frac{1}{1 - r^{-2s}}.$$

En lo que sigue, para simplificar las notaciones, escribiremos

$$s := \sigma + i\tau,$$

con $\sigma, \tau \in \mathbb{R}$.

Sea la función ζ de Riemann

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Como $|n^s| = n^\sigma$, se tiene que es una función analítica en $\sigma > 1$. La función ζ de Riemann admite una extensión analítica a $\mathbb{C}$ excepto $\zeta = 1$, donde la

[11] Esta igualdad utiliza la unicidad de la descomposición en factores primos de un número natural, que la serie $\sum_{n=0}^{\infty} w^n = \frac{1}{1-w}$ converge absolutamente en $|w| < 1$ y que el producto de dos series absolutamente convergentes es absolutamente convergente y el teorema 5.3.

extensión tiene un polo simple. Dicha extensión la seguiremos denotando por ζ.

También, definimos

$$L(s) := \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{(2k+1)^s} = \prod_q \frac{1}{1-q^{-s}} \prod_r \frac{1}{1+r^{-s}},$$

que es una función entera y que en $s = 1$ toma el valor $\frac{\pi}{4}$. Además, L no se anula en un semi-plano de la forma $\Re(s) \geq 1$ (ver[1], pág. 302).

Observar que

$$\prod_q \frac{1}{1-q^{-s}} \prod_r \frac{1}{1+r^{-s}} = \prod_q \sum_{n=0}^{\infty} \frac{1}{q^{ns}} \prod_r \sum_{n=0}^{\infty} \frac{(-1)^n}{r^{ns}}.$$

Por tanto,

$$f(s)^2 = \psi(s)\zeta(s)L(s), \tag{5.7}$$

donde

$$\psi(s) := \frac{1}{1-2^{-s}} \prod_r \frac{1}{1-r^{-2s}}. \tag{5.8}$$

La función ψ es analítica en $\Re(s) > \frac{1}{2}$ porque cada una de las funciones $\frac{1}{1-r^{-2s}}$ lo son y el producto $\prod_r \frac{1}{1-r^{-2s}}$ converge uniformemente en dicha región. Además, cada uno de los factores no se anula, como el límite no es la función idénticamente cero, según el teorema de Hurwitz, la función límite no se anula.

De la relación (5.7) se sigue que existe una función $g(s)$ analítica en un semi-plano $\{s \in \mathbb{C} : \Re(s) > 1 - \theta\}$, para cierto $\theta > 0$ tal que

$$f(s) = (s-1)^{-1/2} g(s), \quad \Re(s) > 1 - \theta \wedge s \notin (-\infty, 1], \tag{5.9}$$

donde tomamos la rama principal de la raíz $(s-1)^{-1/2}$; es decir,

$$(s-1)^{-1/2} := e^{-\frac{1}{2}(\log(|s-1|) + i \arg_{(-\pi,\pi)}(s-1)}.$$

Además,

$$g(1) = \sqrt{L(1)\psi(1)} = \sqrt{\frac{\pi}{2} \prod_r \frac{1}{1-r^{-2}}} = K\sqrt{\pi}.$$

Sea

$$B(x) := \sum_{n \leq x} b_n, \quad x \geq 0.$$

Entonces $B(x)$ representa la cantidad de números menores o iguales que x que son cuadrados o se pueden representar como suma de dos cuadrados.

Extendemos la definición de b_n considerando $b_x = 0$ si $x \in (\mathbb{R} \setminus \mathbb{N})$. Con ello "normalizamos" la definición de B con la siguiente función

$$B^*(x) := \sum_{n<x} b_n + \frac{b_x}{2}, \quad x \geq 0.$$

Según el lema 7.9 con $\kappa > 1$, se cumple

$$B^*(x) = \frac{1}{2\pi i} \int_{\kappa - i\infty}^{\kappa + i\infty} \frac{f(s)x^s}{s} ds,$$

donde la integral es condicionalmente convergente para $x \in \mathbb{R} \setminus \mathbb{N}$ y convergente en el sentido de valor principal de Cauchy para $x \in \mathbb{N}$; así, se tiene

$$B^*(n) = \sum_{j<x} b_j + \frac{b_n}{2} = \lim_{T\to\infty} \frac{1}{2\pi i} \int_{\kappa - iT}^{\kappa + iT} \frac{f(s)n^s}{s} ds. \tag{5.10}$$

Utilizando el teorema de Cauchy, transformamos la curva de integración en (5.10) según el camino en la figura 4. En ese nuevo contorno de integración $\kappa = 2$, dicho contorno está formado por los segmentos que van de $2 - iT$ a $2 + iT$, de $2 + iT$ a $1 + iT$, de $1 + iT$ hasta $1 + i\delta$, un camino que va desde $1 + i\delta$ hasta $1 - \theta + i\epsilon$, el segmento que va de $1 - \theta + i\epsilon$ a $1 + i\epsilon$, la semi-circunferencia de radio ϵ que va de $1 + i\epsilon$ a $1 - i\epsilon$ y que está en el semi-plano $\Re(s) \geq 0$, y el resto del camino de integración es tal que dicho camino es simétrico respecto al eje real, es un camino cerrado y se recorre en sentido positivo. Aquí δ es un número pequeño comparado con T y ϵ es un número positivo pequeño.

La integral "dominante" es

$$\mathcal{I} := \frac{1}{2\pi i} \int_{L^+ + L^-} \frac{f(s)n^s}{s} ds, \tag{5.11}$$

donde $L^{\pm} = [1 - \theta \pm i\epsilon, 1 \pm i\epsilon]$ y θ es un valor positivo pequeño, de modo que $\zeta(s)$ y $L(s)$ no tienen ceros en $\Re(s) \geq 1 - \theta$. Para hacer esta estimación juega un papel importante que

$$|f(s)| \leq C \log(|s|), \quad \Re(s) > 1 - \theta, \tag{5.12}$$

y $|s|$ suficientemente grande.

Por (5.9), si el desarrollo de Taylor de g en $s = 1$ está dado por

$$g(s) = K\sqrt{\pi} + \sum_{j\geq 1} B_j (s-1)^j$$

se tiene que, cuando $\epsilon \to 0$ y $T \to \infty$, que la expresión (5.11) se comporta como

$$\mathcal{I} = \frac{K\sqrt{\pi}}{2\pi i} \int_{L^+ + L^-} \frac{n^s}{(s-1)^{1/2} s} ds + o(\mathcal{I}) = \frac{K}{\sqrt{\pi}} \int_{1-\theta}^{1} \frac{n^s}{(1-s)^{1/2}} ds + o(\mathcal{I}).$$

Haciendo el cambio de variable $1 - s = u$, la integral de la fórmula anterior nos queda

$$\begin{aligned}\int_0^\theta n^{1-u}u^{-1/2}\,du &= \int_0^\theta e^{(1-u)\log(n)}u^{-1/2}\,du = n\int_0^\theta e^{-u\log(n)}u^{-1/2}\,du \\ &= \int_0^{\theta\log(n)} e^{-v}\left(\frac{v}{\log(n)}\right)^{-1/2}\frac{du}{\log(n)} \\ &= \frac{n}{\sqrt{\log(n)}}\left(\Gamma(1/2) - \int_{\theta\log(n)}^\infty e^{-v}v^{-1/2}\,dv\right) \\ &= \frac{n}{\sqrt{\log(n)}}\left(\sqrt{\pi} + O(\int_{\theta\log(n)}^\infty e^{-v}\,dv)\right).\end{aligned}$$

De modo que

$$B(n) \sim B^*(n) \sim K\frac{n}{\sqrt{\log(n)}} \quad cuando \quad n \to \infty.$$

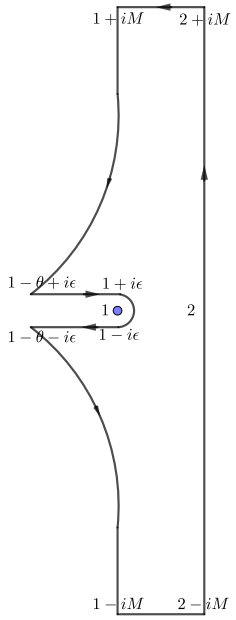


Figura 4: Deformación del contorno de integración en la integral $\frac{1}{2\pi i}\int_{\kappa-iT}^{\kappa+iT}\frac{f(s)n^s}{s}ds$.

□

Ahora, para ver que el conjunto de los números que posiblemente no cumplen la conjetura de Erdös-Straus tiene densidad cero, basta darse cuenta de que como todo número que tiene un factor primo congruente con 3 módulo 4 es un número de Erdös-Strauss, los números para los que posiblemente esta conjetura no es cierta tienen todos sus factores primos congruentes con 1 módulo 4; de modo que ellos son expresables como suma de cuadrados. Y por el teorema 5.4 este conjunto tiene densidad cero.

5.4. Algoritmo

Hemos comprobado que los números n que pertenecen a $\mathcal{N}_1 = \{n \in \mathbb{N} : \exists\, \alpha,\ \beta,\ \gamma \in \mathbb{N}, n = p(\alpha,\ \beta,\ \gamma)\}$ cumplen la conjetura de Erdös-Straus. Para simplificar los cálculos que supondrían generar todos los números pertenecientes a $\mathcal{N}_1$, vamos a generar las clases de equivalencia de tales números, trasladando t unidades cada variable; i.e. las clases de equivalencia

$$N_x = p(x+t,\ y,\ z) = p(x,\ y,\ z) + ((4y+3)(4z+3)-1)t,$$
$$N_y = p(x,\ y+t,\ z) = p(x,\ y,\ z) + 4((x+1)(4z+3)-1)t,$$
$$N_z = p(x+t,\ y,\ z+t) = p(x,\ y,\ z) + 4(x+1)(4y+3)t.$$

Empezando con $x,\ y,\ z \in \{0,\ 1\}$ obtenemos las siguientes clases

$$5+8t,\ 5+12t,\ 13+20t,\ 17+20t,\ 13+28t, 37+52t, \quad t \in \mathbb{N},$$

y después filtramos los números primos congruentes con 1 módulo 4 en estas clases. Mediante cálculos computacionales podemos comprobar si un número pertenece a alguna de las clases que se generan al variar $x,\ y,\ z \in \{0,\ 1, \ldots, N\}$.

6. Biografía

6.1. Paul Erdös

Paul Erdös nació el 26 de marzo de 1913 en Budapest, Hungría, en el seno de una familia judía de profesores de instituto. A pesar de las restricciones antisemitas de las universidades de Hungría, Erdös pudo comenzar sus estudios universitarios con 17 años. Con 19 años hizo su primera aportación a las matemáticas: la demostración del postulado de Bertrand, que afirma que entre cualquier número y su doble siempre existe un número primo.

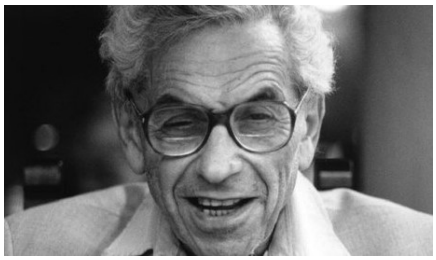
Terminó su doctorado a los 21, para instalarse en Mánchester, Inglaterra y empezar a forjar uno de los rasgos más distintivos de Paul como matemático: un constante peregrinaje de país en país, sin un domicilio ni afiliación permanente a ninguna universidad, y con un desapego absoluto de lo material.

Su vida transcurrió entre viaje y viaje. Falleció con 83 años en plena creación matemática y durante un congreso matemático en Varsovia.

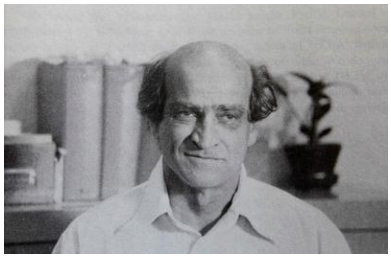
Erdős fue pionero en áreas como la teoría aditiva de los números. También trabajó en aritmética y teoría de números, en análisis matemático, en lógica y especialmente en combinatoria y en teoría de grafos. Fue el matemático más prolífero de toda la historia, sobrepasando al mismísimo Leonhard Euler.

A lo largo de su carrera formuló conjeturas que hoy en día todavía son motivo de investigación matemática. Muy recientemente el medallista Fields Terence Tao presentó una solución al denominado Problema de la discrepancia de Erdős, formulado en el año 1957.

Además, Erdős desarrolló una manera muy personal de hacer ciencia. Él consideraba que la creación era un fenómeno social, y tuvo un gran número de colaboradores científicos en una época en la que el único medio de comunicación era la correspondencia escrita. De hecho, en este contexto se definió un parámetro de colaboración: el número de Erdős, un matemático que ha publicado un artículo con Erdös tiene un número de Erdös de 1. Un matemático que ha publicado un documento con alguien que ha publicado un documento con Erdös tiene un Erdös número de 2, y así sucesivamente. De este modo, un investigador que haya publicado un trabajo conjunto con él tiene número de Erdős igual a 1, un matemático que no haya trabajado con él pero si con un investigador que tenga número 1 tendrá número de Erdős 2, y así de manera sucesiva. Lo sorprendente es que al mirar el número de Erdős de cualquier matemático, dicho valor es siempre muy pequeño, y la mayoría de veces menor que 7.



(a) Paul Erdös, 1913-1983.



(b) Ernst Gabor Straus, 1922-1983.

6.2. Ernst Gabor Straus

Ernst Gabor Straus nació el 25 de febrero de 1922 en Munich, Alemania. Su padre fue un reputado abogado, y su madre fue una de las primeras mujeres que pudieron estudiar medicina oficialmente en una universidad; se graduó en 1905 en la Universidad de Heildelberg. Ernst era el pequeño de cinco hermanos, los cuales fueron criados para apreciar los valores culturales y humanitarios de la sociedad.

Después de la ascensión nazi al gobierno alemán en 1933, la familia Straus emigró a Palestina, donde Ernst fue a la escuela secundaria y a la Universidad Hebrea en Jerusalén. En 1941 ingresó en la Universidad de Columbia para completar sus estudios de postgrado, donde se convirtió en asistente de Albert Einstein y conoció a Paul Erdös. Más tarde, aceptó un puesto de profesor en la Universidad de California en Los Ángeles, donde estuvo hasta la hora de su muerte por un ataque al corazón el 12 de Julio de 1983. Sus estudios iban desde la teoría de la relatividad hasta la teoría de números, particularmente los números trascendentes. Además, durante su vida, Ernst mostró interés en otros campos como la geometría, la teoría de grupos o álgebra lineal.

Ernst apoyó incansablemente a los hombres y mujeres que eran injustamente perseguidos por sus gobiernos por hablar en defensa de la libertad, y también se posicionó en contra de la guerra de Vietnam. Estos valores junto con su capacidad intelectual favorecieron la credibilidad y la imagen de E. G. Straus dentro de la sociedad.

7. Notas adicionales

En estas notas vamos a ver unos resultados necesarios para seguir la demostración del teorema 5.4.

- En la sección 4.4 en [10] se estima la cantidad de números que son suma de dos cuadrados desde A hasta X como

$$K \int_A^X \frac{dt}{\sqrt{\log(t)}}.$$

Veamos que esto es lo mismo que enunciamos nosotros en el teorema 5.4.

Lema 7.1.

$$\int_A^X \frac{dt}{\sqrt{\log(t)}} \sim \frac{X}{\sqrt{\log(X)}} \quad \textit{cuando} \quad X \to \infty.$$

Demostración. Integrando por partes, se tiene que

$$\int_A^X \frac{dt}{\sqrt{\log(t)}} = \frac{X}{\sqrt{\log X}} - \frac{A}{\sqrt{\log A}} + \int_A^X \frac{dt}{2(\log t)^{3/2}}$$

con

$$\begin{cases} u(t) = \frac{1}{\sqrt{\log t}} \Rightarrow u'(t) = -\frac{1}{2t(\log t)^3}, \\ v'(t) = 1 \Rightarrow v(t) = t, \end{cases}$$

y

$$\lim_{X\to\infty} \frac{\int_A^X \frac{dt}{2(\log t)^{3/2}}}{\frac{X}{\sqrt{\log X}}} \overset{\text{L'H}}{=} \lim_{X\to\infty} \frac{\frac{1}{2(\log X)^{3/2}}}{\frac{\sqrt{\log X} - \frac{1}{2(\log X)^{3/2}}}{\log X}} = \lim_{X\to\infty} \frac{\log X}{2((\log X)^2 - \frac{1}{2})} = 0.$$

□

- **Funciones de Dirichlet.** Sea $\{a_n\}$ una sucesión en $\mathbb{C}$. La función de Dirichlet con coeficientes $\{a_n\}$ está dada por

$$A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

para aquellos valores s para los que converge.

Lema 7.2. *Si* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *converge para cierto valor* s_0*, entonces también converge para* $\Re(s) > \Re(s_0)$*. Si* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *converge absolutamente para cierto valor* s_0*, entonces también converge absolutamente para* $\Re(s) > \Re(s_0)$*.*

Nota 7.1. *Podemos encontrar una demostración para este lema en [21], capítulo 2.*

Se llama *abscisa de convergencia* de la serie de Dirichlet a un valor $\sigma_c \in \mathbb{R}$ tal que $A(s)$ está definida si $\Re(s) > \sigma_c$, y abscisa de *convergencia absoluta* a σ_c tal que la serie que define a $A(s)$ converge absolutamente para $\Re(s) > \sigma_a$.

A continuación presentamos varias propiedades de las series de Dirichlet (ver [18]).

Lema 7.3. *Una serie de Dirichlet representa una función analítica en el semi-plano* $\{s \in \mathbb{C} : \Re(s) > \sigma_c\}$*.*

Lema 7.4. *Se tiene que* $\sigma_a \leq \sigma_c + 1$*.*

- **Función zeta de Riemann:**

  Lema 7.5.

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}, \quad \Re(s) > 1. \tag{7.1}$$

  donde el producto se realiza en todos los primos.

  Demostración. Como $p \geq 2$, para $\Re(s) > 1$ se tiene

$$\frac{1}{1 - p^{-s}} = \sum_{n=0}^{\infty} \frac{1}{p^{ns}}.$$

  Si multiplicamos los primos $p = 2, 3, \ldots, P$ (multiplicamos todos los primos hasta P), elevados a ciertas potencias $a_2, a_3, \ldots, a_P$,

$$2^{-a_2 s} 3^{-a_3 s} \ldots P^{-a_P s} = n^{-s},$$

  donde $n = 2^{a_2} 3^{a_3} \ldots P^{a_P}$. Si multiplicamos

$$\prod_{p \leq P} \frac{1}{1 - p^{-s}} = \prod_{p \leq P} \left(\sum_{n=0}^{\infty} \frac{1}{p^{ns}} \right) = \sum_{(P)} n^{-s}$$

tendríamos una suma donde cada n tendría solo factores primos menores o iguales que P. Observar que tal suma incluye todos los naturales hasta P. Por tanto,

$$0 < \sum_{n=1}^{\infty} n^{-\sigma} - \sum_{(P)} n^{-\sigma} < \sum_{n=P+1}^{\infty} n^{-\sigma}.$$

Así que,

$$\sum_{n=1}^{\infty} n^{-\sigma} = \lim_{P\to\infty} \sum_{(P)} n^{-s} = \lim_{P\to\infty} \prod_{p\leq P} \frac{1}{1-p^{-s}}$$

□

Lema 7.6. *La función ζ de Riemann no se anula en $\Im(s) > 1$.*

Demostración. Hemos visto que

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}}, \quad \Re(s) > 1.$$

Ninguno de los factores $1/(1-p^{-s})$ se anula en $\Im(s) > 1$ porque

$$|p^{-s}| = p^{-\Re(s)} < 1 \quad \Re(s) > 1.$$

Por el teorema de Hurwitz, la función limite, $\zeta(s)$, o se anula o es idénticamente cero, pero lo segundo no ocurre.

□

Lema 7.7. *La función ζ de Riemann tiene un polo simple en $s = 1$, con residuo 1. Así,*

$$\zeta(s) = \frac{\widehat{\zeta}(s)}{s-1},$$

donde $\widehat{\zeta}$ es una función entera y $\widehat{\zeta}(1) = 1$.

Nota 7.2. *Podemos encontrar una demostración para este lema en [18], parte II.3.*

- **El producto $\prod_r \frac{1}{1-r^{-2s}}$ representa una función analítica en $\Re(s) > \frac{1}{2}$.**

  Consideremos que $s \in \mathbb{R}$ y $s > 1/2$. Se tiene

$$\prod_{r} \frac{1}{1-r^{-2s}} = \prod_{r} \sum_{n=0}^{\infty} \frac{1}{r^{2ns}}.$$

Como

$$\prod_r \sum_{n=0}^{\infty} \frac{1}{r^{2ns}} \leq \prod_p \sum_{n=0}^{\infty} \frac{1}{p^{2ns}} = \zeta(2s) = \sum_{n=1}^{\infty} \frac{1}{n^{2s}},$$

y como este último converge en $\Re(s) > 1/2$, lo mismo sucede con el primero.

- **Series de Dirichlet. Definición.** Sea $f : \mathbb{N} \to \mathbb{C}$ (se dice que f es una *función aritmética*). La *función de Dirichlet* asociada a f es la función de variable compleja

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}. \tag{7.2}$$

- **Propiedades de las funciones de Dirichlet.**

  Lema 7.8 (Propiedad multiplicativa)**.** *Sean f, g y h funciones aritméticas cuyas funciones de Dirichlet asociadas son F, G y H, respectivamente. Si*

$$h(n) = (f * g)(n) \Leftrightarrow h(n) = \sum_{dd'=n} f(d)g(d'),$$

  Entonces

$$H(s) = F(sG(s)).$$

- **Teorema de Perron.** (Ver [18] pág. 130–134)

  Sea $\{b_n\}$ una sucesión de números complejos y $b_x = 0$ cuando $x \in \mathbb{R}\backslash\mathbb{N}$. Definimos

$$B^*(x) := \sum_{n<x} b_n + \frac{b_x}{2}, \quad x \geq 0.$$

  Lema 7.9 (fórmula de Perron)**.** *Let $\kappa > \max\{0, \sigma_c\}$, donde σ_c es la abscisa de convergencia de $F(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$. Para cada $x > 0$ se cumple*

$$B^*(x) = \frac{1}{2\pi i} \int_{\kappa - i\infty}^{\kappa + i\infty} \frac{F(s)x^s}{s} ds,$$

  donde la integral es condicionalmente convergente para $x \in \mathbb{R} \setminus \mathbb{N}$ y convergente en el sentido de valor principal de Cauchy para $x \in \mathbb{N}$; es decir, se tiene

$$B^*(n) = \sum_{n<x} b_n + \frac{b_n}{2} = \lim_{T\to\infty} \frac{1}{2\pi i} \int_{\kappa - iT}^{\kappa + iT} \frac{F(s)n^s}{s} ds.$$

Demostración. Probamos primero la fórmula de inversión de Perron cuando $\kappa > \sigma_a$. En tal caso, la serie que define F es absoluta y uniformemente convergente cuando $s \geq \kappa$. Por tanto,

$$\frac{1}{2\pi i}\int_{\kappa-i\infty}^{\kappa+i\infty}\frac{F(s)x^s}{s}ds = \frac{1}{2\pi i}\sum_{n=1}^{\infty}a_n\int_{\kappa-i\infty}^{\kappa+i\infty}\left(\frac{x}{n}\right)^s\frac{ds}{s}$$

Aplicando la parte primera del Lema 7.10, cuando $x \in \mathbb{R}\setminus\mathbb{N}$, se obtiene

$$\left|\frac{1}{2\pi i}\int_{\kappa-i\infty}^{\kappa+i\infty}\frac{F(s)x^s}{s}ds - B^*(s)\right| \leq \frac{x^\kappa}{2\pi}(\frac{1}{T}+\frac{1}{T'})\sum_{n=1}^{\infty}\frac{|a_n|}{n^\kappa\log(x/n)}.$$

Sea ahora $\kappa : \sigma_c < \kappa \leq \sigma_a$. Se sabe que $\sigma + 1\sigma_a$, en particular, $\kappa + 1 > \sigma_a$. Consideremos el cuadrado que determinan $\Re(s) = \sigma = \kappa$, $\Re(s) = \kappa + 1$, $\Im(s) = \tau = T$, $\Im(s) = -T$. □

Sea la función

$$h(x) = \begin{cases} 1 & \text{si } x > 1, \\ \frac{1}{2} & \text{si } x = 1, \\ 0 & \text{si } 0 < x < 1. \end{cases}$$

Lema 7.10. *Sea $x > 0$. Para cualesquiera constantes positivas κ, T y T' se cumple:*

1. $$\left|h(x) - \frac{1}{2\pi i}\int_{\kappa-iT'}^{\kappa+iT}\frac{x^s}{s}\,ds\right| \leq \frac{x^\kappa}{2\pi|\log x|}(\frac{1}{T}+\frac{1}{T'}) \quad (x \neq 1),$$

2. $$\left|h(1) - \frac{1}{2\pi i}\int_{\kappa-iT'}^{\kappa+iT}\frac{ds}{s}\right| \leq \frac{\kappa}{T+\kappa}.$$

Conclusiones

A lo largo de este trabajo hemos visto una amplia visión de la conjetura de Erdös-Straus. Para ello, hemos tenido que resolver cuestiones relacionadas con distintos campos de las matemáticas como, estructuras algebraicas, combinatoria, topología y análisis complejo.

Para intentar facilitar la compresión de la conjetura, primero hemos visto una sección donde motivamos el estudio de la misma, seguido de un problema auxiliar que ayudar a comprender la conjetura. Después, hemos presentado la conjetura, y hemos visto distintas propiedades de los números que la cumplen.

Personalmente, durante este trabajo he mejorado la capacidad de trabajo autónomo. También, las pruebas de teoremas y lemas me han exigido aumentar mi rigor como matemático, y darme cuenta de que el estudio de un problema particular puede extenderse casi tanto como se quiera. Además, he observado, que la aplicación de la informática puede complementar un problema matemático concreto.

Referencias

[1] Aposton, T.M. *Introduction to Analytic Number Theory.* Springer-Verlag 1976, pág. 302.

[2] Bello, M. H.; Benito, M.; Fernández E. *On Egyptian fractions*, v1, v2 2014. arXiv:1010.2035v2.

[3] Bleicher, M. N. *A new algorithm for the expansion of Egyptian fracions.* J. Number Theory 4 (1972) 342–382.

[4] Bleicher, M. N.; Erdös, P. *The number of distinct subsums of* $\sum_1^N 1/i$. Math. Comput. 29 (1975) 29–42.

[5] Cohen, H. *Number Theory. I: Tools and Diophantine Equations.* Springer 2007, pág. 314.

[6] Elsholtz, C.; Tao, T. *Counting the number of solutions to the Erdös-Straus equation on unit fractions.* J. Aust Math. Soc. 94 (2013) no. 1, págs. 50–105. arXiv:1107.1010v6.

[7] Eppstein, *D. Egyptian Fractions.*
Web: http://www.ics.uci.edu/eppstein/numth/egypt/.

[8] Fraleigh, V. J. K. *A first course in Abstract Algebra.* Addison-Wesley 1967.

[9] Guy, R. K. *Unsolved problems in number theory.* Springer-Verlag 1994 D11.

[10] Hardy, G. H. *Ramanujan: Twelve lectures on subjects suggested by his life and work*, Cambridge Univ. Press 1940, págs. 9–10, 55, y 60–64.

[11] Hua, L. K. *Introduction to Number Theory*, Springer-Verlag 1982.

[12] Landau, E. *"Über die Einteillung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erfordellichen Quadrate."* Arch. Math. Pys. 13. 1908, págs. 305–312.

[13] Landau, E. *Handbuch der Lehre von der Verteilung der Primzahlen, Bd. II 2nd ed.* New York: Chelsea 1953, págs. 641–669.

[14] Mordell, *L. J. Diophantine Equations.* London: Academic Press, 1969.

[15] Niven, I.; Zuckerman, H. S.; Montgomery, H. L. *An Introduction to Theory of Numbers.* Fith Ed. John Wiley & Sons. 1991.

[16] Rué, J. *El matemático mejor relacionado del mundo.* El país 2017.

[17] Salez. S. *The Erdös-Straus: New modular equations and cheking up to* $N = 10^{17}$. arXiv:1406.6307

[18] Tenenbaum, G. *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.

[19] Varona, J. L. *Recorrido por la teoria de números*, colección «Textos Universitarios», Electolibris – RSME, 2014, págs. 120–133.

[20] Vaughan, R. C. *On a Problem of Erdös, Straus and Schinzel.* Mathematika 17 1970, págs. 193–198.

[21] Widder, D.V. *The Laplacce transform*, Princeton, 1946.

[22] Yamamoto, K. *On the Diofantine Equation* $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ Mem Fac. Sci. Kyushu Univ. Ser. A, V. 19, No. 1 1965, págs. 37–47.